ISSN. 1412-0100 VOL 16, NO 2, OKTOBER 2015

# Steganografi pada Citra dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher

**Ali Akbar Lubis*[1], Ng Poi Wong[2], Irfan Arfiandi[3], V. Immanuel Damanik[4], Adithya Maulana[5]**
STMIK Mikroskil, Jl. Thamrin No. 112, 124, 140, Telp. (061) 4573767, Fax. (061) 4567789
[1,2,3,4,5]Jurusan Teknik Informatika, STMIK Mikroskil, Medan
*[1]ali.akbar@mikroskil.ac.id, [2]poiwong@mikroskil.ac.id, [3]111111098@students.mikroskil.ac.id,
[4]111112697@students.mikroskil.ac.id, [5]111111101@ students.mikroskil.ac.id

***Abstrak***

*Least Significant Bit (LSB) merupakan salah satu metode steganografi. Dari segi kapasitas, metode ini hanya mampu menampung sedikit pesan, ini karena LSB hanya menggunakan 3 bit disetiap pikselnya. Dari segi keamanan juga sangat mudah untuk diekstrak oleh steganalis, karena pesan yang disisip terdapat disetiap bit terakhir RGB di setiap piksel dari stego image tanpa adanya enkripsi terhadap pesan terlebih dahulu. Sebuah metode berprinsip sama dengan LSB dengan peningkatan keamanan dan kapasitas menggunakan metode Modified Least Significant Bit (MLSB) yang dikombinasi dengan teknik enkripsi triple transposition vigenere cipher. MLSB merupakan metode LSB yang telah dimodifikasi dengan mengubah data dari bilangan 8 bit menjadi 5 bit, kemudian disisipkan ke dalam cover image. Teknik triple transposition vigenere cipher juga merupakan modifikasi dari teknik vigenere cipher dengan melakukan proses substitusi dan transposisi sebanyak 3 kali dengan kunci yang berbeda satu sama lain. Hasil pengujian menunjukkan bahwa kecepatan dan kualitas citra hasil steganografi bergantung pada berapa banyak karakter dan keacakan dari karakter yang akan diinput. Kualitas citra steganografi dengan metode ini menunjukkan kualitas yang baik, karena nilai PSNR di atas 40dB. file citra sebelum dan sesudah disisipi pesan, tidak menunjukkan perbedaan yang signifikan dan pesan yang diekstrak tidak mengalami perubahan.*

***Kata kunci***— *Steganografi, Modified Least Significant Bit, Triple Transposition Vigenere Cipher.*

***Abstract***

*Least Significant Bit (LSB) is one of steganography method. From the capacity, this method can only accomodate few message, because LSB only using 3 bits at each of the pixel. In terms of security it is really easy to extract by steganalis, because the message that was inserted can be found in every end of bits RGB in every pixel of stego image without encryption to the message before. The method that have same principle with LSB with enhancement of security and capacity using Modified Least Significant Bit (MLSB) method will combine with triple transposition vigenere cipher encryption technique. MLSB is a modified LSB method by changing the data from 8 bit into 5 bits, then inserted into cover image. Triple transposition vigenere cipher technique is a modified vigenere cipher technique with the substitution and transposition process as much as 3 times with the key that differ from one another. The test results showed that the speed and quality of image steganography depend on how much the character and the randomness of the character which will inputted. Image steganografi quality with this method showed a good quality, because the PSNR value above 40db. Image file before and after message inserted, did not show any significant difference and the message that have been extracted is unchanged.*

***Keywords***— *Steganography, Modified Least Significant Bit, triple transposition vigenere cipher.*

## 1. PENDAHULUAN

Steganografi merupakan seni penyimpanan pesan rahasia dengan menggunakan media digital seperti teks, citra, suara dan video. Data yang tersembunyi didalam steganografi merupakan hal yang sulit untuk dideteksi dan bila dikombinasikan dengan algoritma yang cocok maka akan lebih sulit untuk diuraikan [1]. Ada berbagai macam metode untuk steganografi, salah satunya adalah metode metode Modified Least Significant Bit (MLSB). Memperkenalkan modifikasi yang lebih baik dari metode Least Significant Bit (LSB), untuk meningkatkan perlindungan data. Pada metode LSB, data yang disisipkan merupakan bilangan 8 bit tanpa adanya proses enkripsi terlebih dahulu, sehingga lemah dalam keamanannya [2]. Metode Modified Least Significant Bit (MLSB) telah ditambahkan teknik enkripsi sederhana di dalam algoritmanya. Teknik enkripsi yang ditambahkan adalah mengkonversi data yang terdiri dari 8 bit menjadi 5 bit. Sebagai modifikasi dari metode LSB, output gambar dari metode MLSB ini akan terlihat sama dengan cover image [3]. Penelitian ini juga menambahkan teknik enkripsi triple transposition vigènere cipher, yang merupakan metode enkripsi dengan cara mengulang teknik vigènere cipher dimana setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang berbeda satu dengan yang lainnya. Kelebihan dari teknik ini adalah kekuatan enkripsinya sekuat one time pad, karena diklaim tidak dapat dipecahkan dengan menggunakan exhautisve key search attack [4].

Tujuan dari penelitian ini adalah untuk menghasilkan sebuah aplikasi penyembunyian pesan ke dalam media gambar dengan menggunakan algoritma Modified Least Significant Bit (MLSB) dan enkripsi triple transposition vigenere cipher, sedangkan manfaatnya agar diperolehnya peningkatan kualitas pengamanan sebuah data.

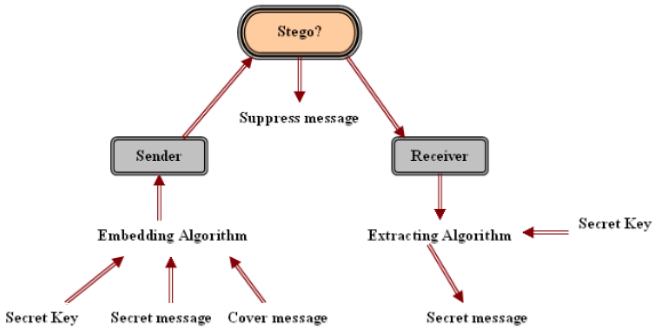
Data yang dapat disisipkan ke dalam file citra adalah pesan teks dimana karakter yang dapat disisipkan berupa printable characters (karakter dengan kode ASCII 20h – 7Eh). Media yang digunakan dalam menyisipkan pesan teks berupa file citra RGB dengan format BMP, JPG dan PNG dimana output berupa file citra dengan format PNG, dan lokasi penyimpanan file dapat ditentukan secara manual oleh user. Panjang pesan teks dibatasi dengan ukuran file citra dan panjang kunci minimal 3 karakter dan maksimal sesuai panjang pesan teks.

## 2. METODE PENELITIAN

### 2.1. Tinjauan Pustaka

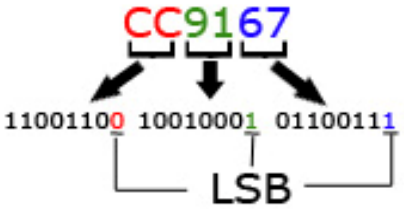
#### 2.1.1. Modified Least Significant Bit (MLSB)

Steganografi berasal dari kata Yunani yang berarti tulisan tersembunyi. Kata steganografi diklasifikasikan menjadi dua bagian yaitu *steganos* yang berarti rahasia atau tertutup dan *grafis* yang berarti menulis. Namun, dalam menyembunyikan informasi, makna steganografi adalah menyembunyikan pesan teks atau pesan rahasia ke dalam file media lain seperti gambar, teks, suara, dan video. Terminologi utama yang digunakan dalam sistem steganografi adalah media penyisipan, pesan rahasia, kunci rahasia dan algoritma penyisipan [5].




Gambar 1. *Steganography system scenario* [5]

Metode *Modified Least Significant Bit* (MLSB) adalah suatu metode dari hasil pengembangan metode LSB yang sudah ada. Pada metode MLSB ini, bilangan yang di pakai adalah bilangan 5 bit hasil konversi dari bilangan 8 bit yang dipakai pada metode LSB [2]. Kemudian bilangan 5 bit disisipkan ke dalam *cover image* menggunakan metode LSB. Bit yang diganti di dalam metode LSB ini, adalah bit terakhir yang diganti dengan bit dari pesan teks. Teknik ini bekerja baik untuk steganografi gambar, khususnya pada mata manusia karena *stego image* akan terlihat sama dengan *cover image*-nya. Untuk menyembunyikan informasi ke dalam gambar, metode LSB biasanya banyak digunakan. File gambar yang telah distego akan menunjukkan perbedaan warna dan intensitas cahaya yang kecil pada suatu bidang gambar [6].




Gambar 2. Steganografi pada citra RGB [7]

Pada Gambar 2 terlihat bit-bit LSB pada 1 piksel warna, penyisipan informasi dapat dilakukan pada bit-bit tersebut [7].

### 2.1.2. Triple Transposition Vigenere Cipher

*Triple transposition vigenere cipher* adalah metode enkripsi dengan cara mengulang teknik *vigènere cipher* yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya [4]. *Triple transposition vigenere cipher* terbagi menjadi dua bagian yaitu metode transposisi dan metode substitusi. Metode transposisi dapat disimbolkan dengan T dan metode substitusi menggunakan *vigenere* yang disimbolkan dengan S serta kunci untuk melakukan teknik *vigenere*. Secara matematis metode *triple transposition vigenere cipher* ini dapat dituliskan sebagai:

**Proses enkripsi**: C = S3 (T3 (S2 (T2 (S1 (T1 (P)))))) (1)

Proses dekripsi dapat dilakukan dengan arah sebaliknya. Bila dirumuskan maka akan terlihat sebagai berikut:

**Proses dekripsi**: P = T1'(S1'(T2'(S2'(T3'(S3'(C)))))) (2)

Maksud T' disini adalah transposisi kebalikkannya dan S' adalah substitusi kebalikannya. Pada teknik ini, tabel *vigenere cipher* juga mengalami modifikasi di bagian daya tampung plainteks dan kuncinya. Jika sebelumnya pada teknik *vigenere cipher* hanya bisa menampung plainteks dan kunci yang terdiri dari huruf A – Z, maka pada teknik *triple transposition vigenere cipher* tabel *vigenere* di modifikasi sehingga plainteks dan kunci dapat menampung *printable character* (karakter dengan kode ASCII 20h – 7Eh). Teknik ini juga dapat dikombinasikan dengan metode steganografi *Modified Least Significant Bit* (MLSB), karena mempunyai batasan masalah yang sama, yaitu hanya dapat menampung *printable character* (karakter dengan kode ASCII 20h – 7Eh).

## 2.2. Analisis

### 2.2.1. Analisis Algoritma Modified Least Significant Bit (MLSB)

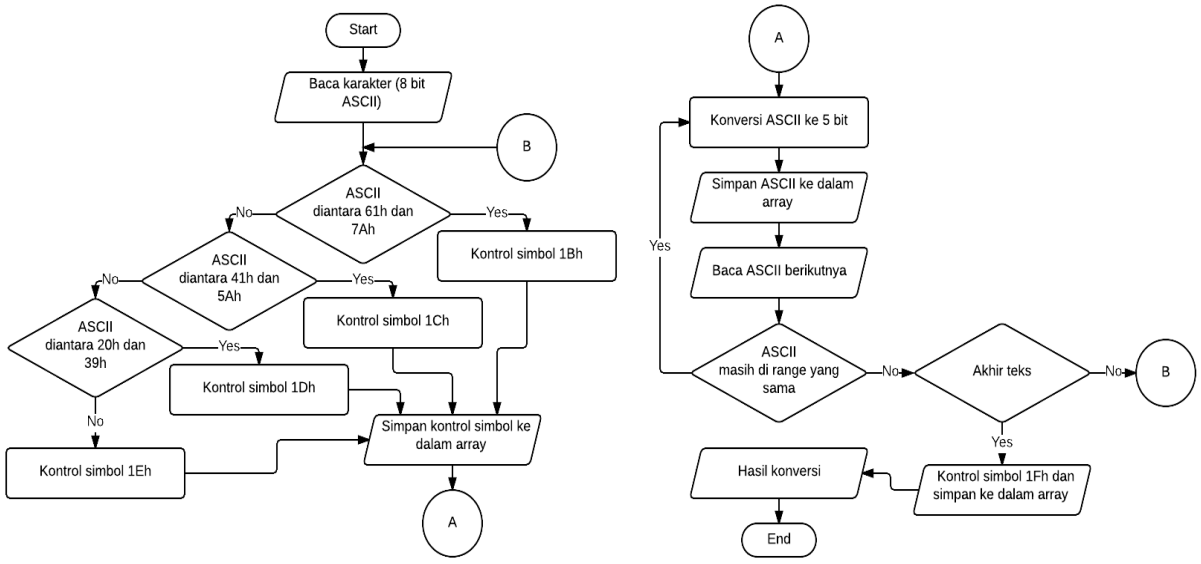
Adapun cara kerja algoritma Modified Least Significant Bit (MLSB) adalah sebagai berikut:

1. 61h – 7Ah (*Small Letter*)

Jika kode ASCII dari karakter yang disisip diantara 61h – 7Ah, pertama harus menempatkan 1Bh di awal, selanjutnya memasukkan karakter yang telah dikonversi dari bilangan 8 bit menjadi 5 bit. Kemudian konversi karakter berikutnya jika berada di *range* yang sama.

2. 41h – 5Ah (*Capital Letter*)
   Jika kode ASCII dari karakter yang disisip diantara 41h – 5Ah, pertama harus menempatkan 1Ch di awal, selanjutnya memasukkan karakter yang telah dikonversi dari bilangan 8 bit menjadi 5 bit. Kemudian konversi karakter berikutnya jika berada di *range* yang sama.
3. 20h – 39h
   Jika kode ASCII dari karakter yang disisip diantara 20h – 39h, pertama harus menempatkan 1Dh di awal, selanjutnya memasukkan karakter yang telah dikonversi dari bilangan 8 bit menjadi 5 bit. Kemudian konversi karakter berikutnya jika berada di *range* yang sama.
4. 3Ah – 40h, 5Bh – 60h, 7Bh – 7Eh atau Ah (*Enter*)
   Jika kode ASCII dari karakter yang disisip diantara 3Ah – 40h, 5Bh – 60h, 7Bh – 7Eh atau Ah, pertama harus menempatkan 1Eh di awal, selanjutnya memasukkan karakter yang telah dikonversi dari bilangan 8 bit menjadi 5 bit. Kemudian konversi karakter berikutnya jika berada di *range* yang sama.
5. Akhir Teks
   Untuk menandakan teks telah berakhir, maka harus disisipkan 1Fh.

*Flowchart* dari metode *Modified Least Significant Bit* (MLSB) dapat dilihat pada Gambar 3:

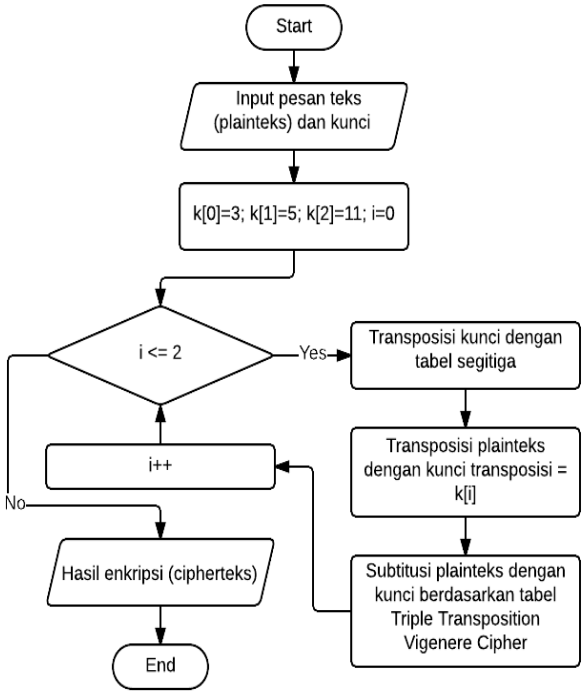



*Gambar 3. Flowchart Modified Least Significant Bit (MLSB).*

Pada Gambar 3 dijelaskan proses kerja dari metode *Modified Least Significant Bit* (MLSB) dimana data di konversi dari 8 bit menjadi 5 bit. Pertama baca karakter (8 bit) lalu tentukan kode ASCII karakter untuk menentukan kontrol simbol sebagai penanda jenis karakter berikutnya. Lakukan proses konversi sampai karakter terakhir, dimana kontrol simbol 1Fh digunakan sebagai tanda akhir teks.

### 2.2.2. Analisis Algoritma Triple Transposition Vigenere Cipher

Pada teknik Triple Transposition Vigenere Cipher, tabel bujursangkar vigenere cipher ditambahkan jumlah karakter sehingga dapat menampung *printable character* (karakter dengan kode ASCII 20h – 7Eh). Flowchart dari teknik enkripsi *triple transposition vigenere cipher* dapat dilihat pada Gambar 4 berikut:




Gambar 4. *Flowchart* proses enkripsi *triple transposition vigenere cipher*.

Pada Gambar 4 dijelaskan penyisipan pesan teks dan kunci untuk melakukan proses enkripsi menggunakan *triple transposition vigenere cipher*, setelah itu dilakukan proses inisialisasi kunci transposisi *triple transposition vigenere cipher*. Lakukan proses transposisi kunci dengan tabel segitiga, lalu lakukan transposisi plainteks dengan kunci transposisi = k[i]. Setelah itu lakukan substitusi plainteks dengan kunci berdasarkan tabel *triple transposition vigenere cipher*. Kemudian lakukan proses tersebut sampai plainteks terakhir lalu tampilkan hasil enkripsi (cipherteks).

Adapun cara kerja algoritma ini untuk mendapatkan cipherteks dapat dilihat dari source code pada Gambar 5 berikut:

```
cipherteks = (ASII_karakter_pesan + ASCII_karakter_kunci -32) % 127

if (ASII_karakter_pesan + ASCII_karakter_kunci - 32) / 127)>= 1
cipherteks = (ASII_karakter_pesan + ASCII_karakter_kunci) % 127
```

Gambar 5. Algoritma enkripsi *triple transposition vigenere cipher*

Pada Gambar 5 dijelaskan untuk mendapatkan cipherteks dari pesan dan kunci, maka lakukan perhitungan (ASCII_karakter_pesan + ASCII_karakter_kunci – 32) mod 127. Periksa nilai perhitungan dari (ASCII_karakter_pesan + ASCII_karakter_kunci – 32) / 127), jika hasil perhitungan di bawah atau sama dengan 1, maka untuk mendapatkan cipherteks harus menggunakan perhitungan yang berbeda yaitu (ASCII_karakter_pesan + ASCII_karakter_kunci) mod 127.

### 2.2.3. Metode Analisis Hasil

Kualitas gambar yang baik dari file citra steganografi merupakan syarat utama dari kesuksesan algoritma steganografi. Salah satu cara untuk menghitung nilai kualitas dari file citra steganografi menggunkan rumus *Means Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR). *Means*

*Square Error* (MSE) adalah rata-rata kuadrat nilai kesalahan antara citra asli dengan citra manipulasi [8]. Secara matematis dapat ditulis seperti persamaan 3:

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left|\left(f(x,y)-g(x,y)\right)^2\right| \quad (3)$$

Semakin rendah nilai MSE maka akan semakin baik. Setelah diperoleh nilai MSE maka nilai *Peak Signal to Noise Ratio* (PSNR) dapat dihitung, yang dimana PSNR adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan desibel, PSNR digunakan untuk mengetahui perbandingan kualitas *cover image* sebelum dan sesudah disisipkan pesan [8]. Secara matematis dapat ditulis seperti persamaan 4.

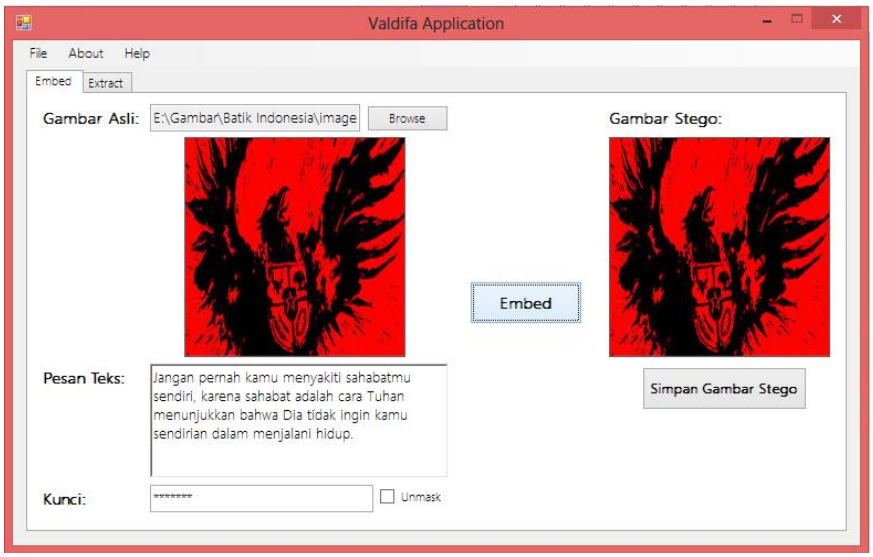
$$PSNR = 10\log_{10}\left(\frac{C_{max}^2}{MSE}\right) \quad (4)$$

Semakin besar nilai PSNR maka akan semakin baik kualitas citra steganografi. Kualitas citra dapat disimpulkan cukup baik jika nilai PSNR memnuhi standar yaitu di atas 30dB – 40dB [9].

## 3. HASIL DAN PEMBAHASAN

### 3.1 Hasil

Hasil penelitian yang diperoleh dari uji coba aplikasi yang sudah dibuat terlihat pada gambar 6 dan 7 untuk proses e*mbedding* dan e*xtracting* pesan. Form *embedding* digunakan untuk melakukan proses penyisipan pesan ke dalam *cover image*. Adapun tampilan dari form *embedding* seperti Gambar 6 berikut:

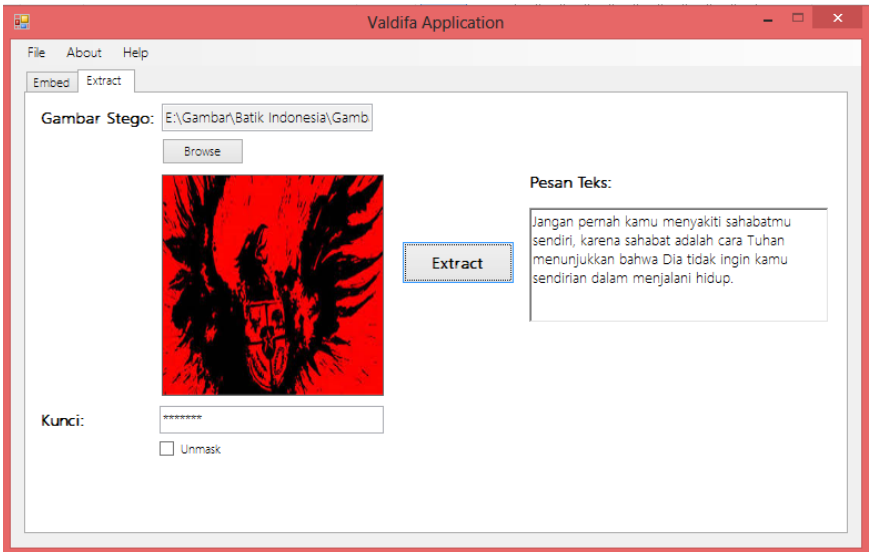



Gambar 6. Form *embedding*

Pada Gambar 6 menunjukkan tampilan dari form *embedding*. Cara kerja pada form ini pertama-tama pilih *cover image* yang akan digunakan untuk menyimpan pesan. Untuk memilih *cover image*, maka klik *button browse*, kemudian *input* pesan dan *password*. Setelah semua data dimasukkan, klik *tombol embed* sehingga sistem akan menyisipkan pesan rahasia ke dalam *cover image*. Setelah proses penyisipan selesai, maka *stego image* akan tampil pada *picturebox*, terdapat juga

*button* simpan gambar di bawahnya. *User* dapat meng-klik *button* simpan gambar untuk menyimpan *stego image*.

Form *extrcacting* digunakan untuk melakukan proses ekstraksi pesan dari dalam *stego image*. Adapun tampilan dari form *extrcacting* seperti Gambar 7 berikut:



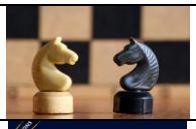

Gambar 7. Form *extraction*

Pada Gambar 7 menunjukkan tampilan dari form *embedding*. Cara kerja pada form ini diawali dengan memilih *stego image* dan *input password*. *Password* yang dimasukkan harus sama dengan *password* yang digunakan pada saat proses *embed*, kemudian klik *button extract*. Setelah proses ekstraksi selesai, maka pesan akan muncul di *textarea*.

### 3.2 Pembahasan

Pengujian yang dilakukan terhadap aplikasi yang dibangun adalah mengukur tingkat kualitas dari file citra sebelum dan sesudah disisipkan pesan dengan kombinasi dari resolusi gambar yang bervariasi dan jumlah karakter pesan yang bervariasi.

Tabel 1. Kelima *cover image* yang digunakan dalam proses pengujian

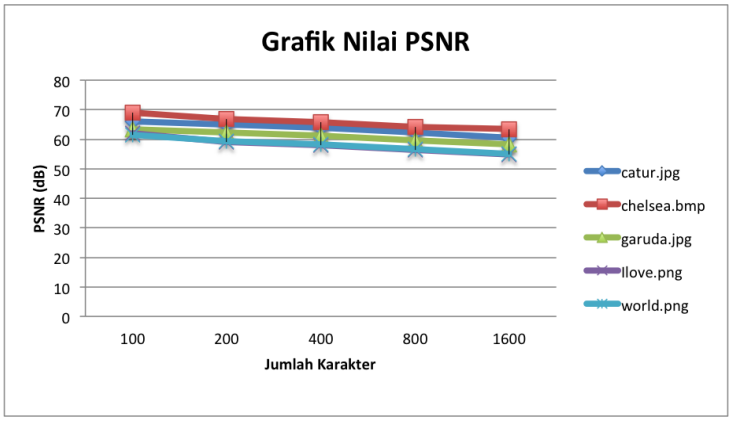
| No | Nama Gambar | Gambar | Resolusi Gambar | No | Nama Gambar | Gambar | Resolusi Gambar |
|---|---|---|---|---|---|---|---|
| 1 | catur.jpg |  | 1024 x 7680 piksel | 4 | ilove.png |   | 267 x 189 piksel |
| 2 | chelsea.bmp |   | 1680 x 1050 piksel | 5 | world.png |  | 300 x 194 piksel |
| 3 | garuda.jpg |  | 600 x 375 piksel | | | | |

Pengujian yang dilakukan menggunakan metode *Modified Least Significant Bit* (MLSB) dan enkripsi *triple transposition vigenere cipher* kemudian dihasilkan nilai MSE, PSNR dan waktu eksekusi yang dapat dilihat pada Tabel 2 berikut:

Tabel 2. Nilai MSE, PSNR dan waktu eksekusi program

| ***Cover Image*** | **Karakter** | **PSNR (dB)** | **Waktu Sisip (*second*)** | **Waktu Ekstrak (*second*)** |
|---|---|---|---|---|
| catur.jpg | 100 | 66,15 | 0,011 | 0,002 |
| | 200 | 64,98 | 0,013 | 0,003 |
| | 400 | 63,93 | 0,015 | 0,005 |
| | 800 | 62,3 | 0,018 | 0,007 |
| | 1600 | 60,5 | 0,023 | 0,015 |
| chelsea.bmp | 100 | 68,9 | 0,026 | 0,002 |
| | 200 | 66,86 | 0,028 | 0,003 |
| | 400 | 65,89 | 0,031 | 0,004 |
| | 800 | 64,28 | 0,035 | 0,007 |
| | 1600 | 63,48 | 0,039 | 0,014 |
| garuda.jpg | 100 | 63,38 | 0,003 | 0,002 |
| | 200 | 62,32 | 0,004 | 0,003 |
| | 400 | 61,21 | 0,006 | 0,004 |
| | 800 | 59,59 | 0,009 | 0,007 |
| | 1600 | 58,16 | 0,015 | 0,014 |
| ilove.png | 100 | 61,92 | 0,001 | 0,002 |
| | 200 | 59,04 | 0,002 | 0,003 |
| | 400 | 57,89 | 0,006 | 0,004 |
| | 800 | 56,35 | 0,008 | 0,006 |
| | 1600 | 54,85 | 0,01 | 0,014 |
| world.png | 100 | 61,45 | 0,001 | 0,002 |
| | 200 | 59,36 | 0,002 | 0,003 |
| | 400 | 58,28 | 0,003 | 0,005 |
| | 800 | 56,96 | 0,007 | 0,007 |
| | 1600 | 54,99 | 0,014 | 0,018 |

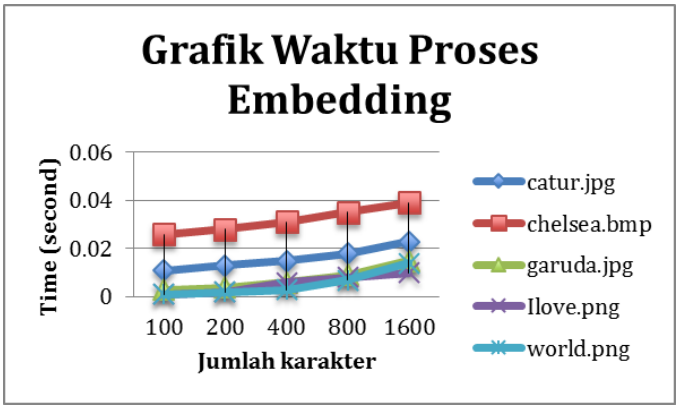
Pengujian pertama yang dilakukan adalah untuk mengukur tingkat kualitas dari gambar sebelum dan sesudah disisipkan pesan dengan resolusi gambar yang bervariasi dan jumlah karakter pesan yang bervariasi. Hasil dari pengujian yang pertama dapat dilihat pada grafik pada Gambar 8 berikut:




Gambar 8. Grafik nilai PSNR

Dari grafik pada Gambar 8 dapat dilihat bahwa jumlah karakter pesan yang disisipkan pada setiap *cover image* berpengaruh terhadap nilai PSNR yang dihasilkan atau dengan kata lain semakin banyak karakter pesan yang disisipkan ke dalam *cover image*, maka semakin berkurang juga kualitas dari gambar yang dihasilkan. Hal ini ditandai dengan berkurangnya nilai PSNR yang dihasilkan oleh masing-masing *stego image* dengan jumlah karakter pesan yang bervariasi.

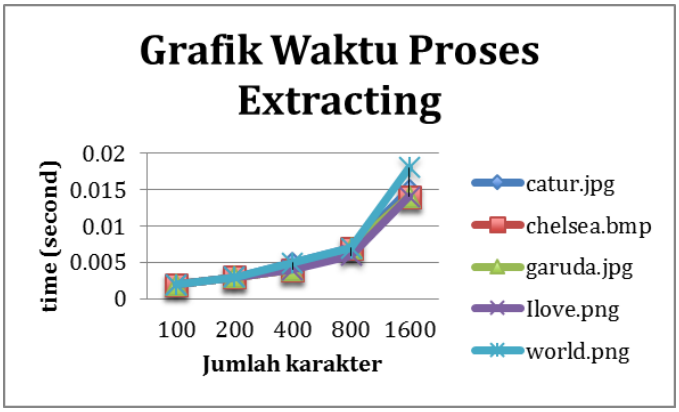
Pengujian kedua yang dilakukan adalah untuk mengukur waktu eksekusi program di dalam proses penyisipan pesan dengan resolusi gambar yang bervariasi dan jumlah karakter pesan yang bervariasi. Hasil dari pengujian yang pertama dapat dilihat pada grafik pada Gambar 9 berikut:




Gambar 9. Grafik waktu proses *embedding*

Dari grafik pada Gambar 9 dapat dilihat bahwa jumlah karakter pesan mempengaruhi lamanya waktu pada proses penyisipan. Karena bertambahnya jumlah karakter pesan membuat sistem lama dalam mengihung banyaknya bit pesan yang akan disisipkan ke dalam *cover image*.

Pengujian ketiga yang dilakukan adalah untuk mengukur waktu eksekusi program di dalam proses ekstraksi pesan dengan resolusi gambar yang bervariasi dan jumlah karakter pesan yang bervariasi. Hasil dari pengujian yang pertama dapat dilihat pada grafik pada Gambar 10.




Gambar 10. Grafik waktu proses *extracting*

Dari grafik pada Gambar 10 dapat dilihat bahwa jumlah karakter pesan juga mempengaruhi lamanya waktu pada proses ekstraksi pesan. Proses estraksi pesan yang lama terjadi karena sistem harus mendeteksi banyaknya bit pesan yang kemudian dikonversi menjadi karakter.

## 4. KESIMPULAN

Dari hasil pengujian yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Dengan metode *Modified Least Significant Bit* (MLSB) dan enkripsi *triple transposition vigenere cipher*, kualitas citra dari *stego image* dapat disimpulkan citra yang baik karena menunjukkan nilai PSNR di atas 40dB.
2. Metode *Modified Least Significant Bit* (MLSB) dan enkripsi *triple transposition vigenere cipher* ini juga menunjukkan waktu eksekusi program pada proses penyisipan dan ekstraksi pesan tidak membutuhkan waktu yang terlalu lama.

## 5. SARAN

Adapun saran yang dapat diberikan untuk pengembangan sistem lebih lanjut adalah sebagai berikut:

1. Dapat menyembunyikan pesan teks ke dalam media audio ataupun video dengan metode *Modified Least Significant Bit* (MLSB).
2. Metode *Modified Least Significant Bit* (MLSB) dapat dikembangkan dengan menggunakan metode skema penyisipan seperti *spiral*, *square*, *snake* dan lain sebagainya dalam menyisipkan pesan.
3. Menambahkan teknik enkripsi seperti AES 256 dan lain sebagainya pada metode *Modified Least Significant Bit* (MLSB), sehingga pesan yang disisipkan memiliki tingkat keamanan yang lebih baik.

## DAFTAR PUSTAKA

[1] Channalli, S., 2009, Steganography An Art Of Hiding Data, *International Journal on Computer Science and Enginering*, Vol. 1, hal 137-141

[2] Nimje, S., Belkhede, A., Chaudari, G., Pawar, A., Kharbikar, K., 2014, Hiding Existence of Communication Using Image Steganography, International Journal of Computer Science and Engineering, Vol. 2, hal. 163-166.

[3] Zaher, M. A., 2011, Modified Least Significant Bit (MLSB), Computer and Information Science, Vol. 4, No. 1, hal. 60-67.

[4] Caroline, M. L., 2011, Metode Enkripsi Baru: Triple Transposition Vigenere Cipher

[5] Al-Shatnawi, A. M., 2012, A New Method in Image Steganography with Improved Image Quality, Applied Mathematical Sciences, Vol.6, No. 79, hal. 3907-3915.

[6] Alatas, P., 2009, Implementasi Teknik Steganografi dengan Metode LSB pada Citra Digital, Skipri, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Gunadarma, Jakarta.

[7] Susanti, I., 2007, Penerapan Steganografi Gambar Pada Least Significant Bit (LSB) Dengan Penggunaan PRNG (Pseudo Number Generator), *Skripsi*, Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor, Bogor.

[8] Male, G. M., Wirawan, Setijadi, E., 2012, Analisa Kualitas Citra pada Steganografi untuk Aplikasi e-Government, *Prosiding Seminar Nasional Manajemen Teknologi XV*, Surabaya, Februari 4.

[9] Suhartono, D., Salman, A. G., Rojali, Octavianus, C., 2012, Aplikasi Penyembunyian Pesan pada Citra JPEG dengan Algoritma F5 dalam Perangkat Mobile Berbasis Android. *Seminar Nasional Aplikasi Teknologi Informasi 2012*, Yogyakarta, June 15-16.