Jurnal Ilmiah Matematika dan Terapan
Volume 15 Nomor 2 Desember 2018 (Halaman 268 - 279)

JIMT
Jurnal Ilmiah Matematika dan Terapan

ISSN : 2450 – 766X

RANCANG BANGUN APLIKASI *STEGANOGRAPHY* METODE *MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT* (MELSBR)

I. Aprilia[1], D. Ariyanti[2] dan A. Izzuddin[3]

[1,2,3]Program Studi Teknik Elektro Fakultas Teknik Universitas Panca Marga Prooblinggo
Jl. Yos Sudarso No. 107 Pabean Dringu Probolinggo 67271
[1]Ira.aprilia11@upm.ac.id, [2]dekd19@yahoo.com, [3]ahmad.izzuddin@upm.ac.id

ABSTRACT

Digital data security today is an important part of user because of the increasingly widespread misuse of individuals who can easily open a personal thing. In this case, steganography is a technique that discusses the security of digital data information through the technique of hiding data into other data. Many methods are used in steganography techniques in the process of hiding digital data information. But in this study, the author uses the steganography method based on the insertion of files in the form of files, namely in this case * txt file using the Minimum Error Least Significant Bit Replacement (MELSBR) method with a media storage in the form of 24-bit bitmap files and data that can be inserted in the form of files * txt. The nature of the MELSBR method is to adapt to the local characteristics of the storage medium. In the process of image processing testing researchers use PSNR parameters to determine the quality comparison of digital images before and after processing. The results of this study, concealment and insertion using the MELSBR method with PSNR testing has a greater value so that it can be concluded that the image after processing is getting closer to the cover image.

Keyword : Image Processing, Minimum Error Least Significant Bit Replacement (MELSBR), Steganography.

ABSTRAK

Keamanan data digital dewasa ini adalah salah satu bagian penting dari penggunaan komputer karena semakin maraknya penyalahgunaan oknum-oknum yang dapat membuka dengan mudah suatu hal yang bersifat pribadi. Dalam hal ini, steganografi merupakan teknik yang membahas mengenai pengamanan infromasi data digital lewat teknik penyembunyian data kedalam data yang lainnya. Banyak metode yang digunakan dalam teknik steganography dalam proses penyembunyian informasi data digital. Namun pada penelitian ini, Penulis menngunakan metode steganography berdasarkan penyisipan file berupa berkas yaitu dalam hal ini file *txt dengan mengggunaka metode *Minimum Error Least Significant Bit Replacement* (MELSBR) dengan penampungan media yang berupa berkas bitmap 24 bit serta data yang dapat disisipkan berupa berkas *txt. Sifat dari metode MELSBR ini adalah beradaptasi dengan karakteristik lokal dari media penampung. Pada proses pengujian pemrosesan citra peneliti menggunakan parameter PSNR untuk mengetahui perbandingan kualitas citra digital sebelum dan sesudah diproses. Adapun hasli dari penelitian ini, penyembunyian serta penyisipannya menggunakan metode MELSBR dengan pengujian PSNR bernilai semakin besar sehingga dapat disimpulkan bahwa citra setelah diproses semakin mendekati citra slinya.

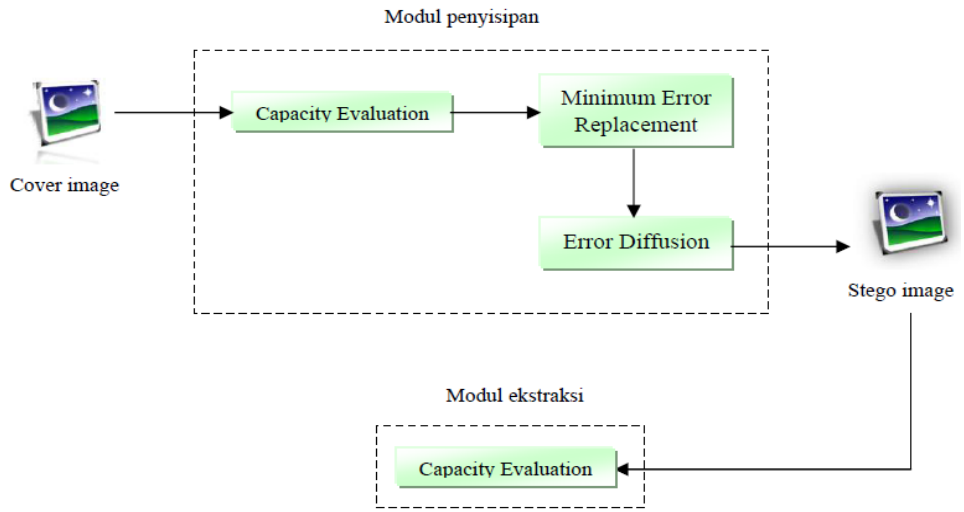
Keyword : Citra digital, Minimum Error Least Significant Bit Replacement (MELSBR), Steganografi.

I. LATAR BELAKANG

1.1. Latar Belakang

Pada era sekarang ini, semakin berkembangnya teknologi komputer maka semakin marak pula kegiatan saling bertukar informasi, data dan pesan bagi penggunaan komputer di dunia ini dengan hal-hal yang bersifat pribadi. Salah satu bagian terpenting dalam teknologi internet yaitu keamanan informasi data digital agar tidak terjadi suatu penyalahgunaan oknum-oknum yang tidak bertanggung jawab. Keamanan merupakan bagian dari perlindungan informasi yang dapat mengamankan data dari penyerang yang ingin mencuri informasi data. Dalam hal ini, sistem keamanan memiliki dua bagian yang kriptografi dan penyembunyian informasi [1]. Adapun cara yang digunakan dalam keamanan data digital yaitu dengan menggunakan teknik steganografi. Steganografi merupakan seni untuk menyembunyikan pesan di dalam media digital sedemikian rupa, sehingga orang lain tidak menyadari ada suatu pesan di dalam media tersebut. Steganografi membutuhkan dua properti yaitu wadah penampug dan data rahasia yang disembunyikan [2].

Metode yang terdapat pada teknik steganografi ini banyak sekali yang bisa digunakan dalam penyembunyian pesan. Metode lain yang dikembangkan dalam penelitian ini adalah metode MELSBR. Metode ini pertama kali diperkenalan oleh Yeuan-Keun Lee dan Ling-Hwein Chen dimana dalam makalahnya mengenai *An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement*. Metode MELSBR yang diterapkan pada citra berwarna (bitmap 24-bit) memiliki beberapa langkah atau tahapan utama untuk melakukan proses penyisipan, antara lain *Capacity Evaluation, Minimum Error Replacement dan Error Diffusion* [3]. Adapun gambaran umum dari metode yang diajukan adalah seperti pada Gambar 1.



Gambar 1 : Gambaran Umum MELSBR [2]

Proses pengujian dalam penelitian ini dilkukan dengan perhitungan PSNR digunakan untuk membandingkan kualitas citra hasil dengan citra asal. Semakin tinggi nilai PSNR maka semakin bagus kualitas citra tersebut [4].

Permasalahan yang akan diangkat oleh peneliti yaitu mengimplementasikan algoritma yang ada dalam kasus penyembunyian pesan rahasia dalam citra digital dengan merancang bangun aplikasi steganografi. Dalam kasus penelitian ini, akan dilakukan proses penyembunyian pesan digital dengan media penampung suatu berkas file gambar berupa bitmap 24 bit dengan penyisipan file berupa *text dengan menggunakan Metode MELSBR dengan pengujian PSNR membandingkan citra asli dengan stego image yang sudah diperoleh dari hasil penyisipan file text.

1.2. Batasan Masalah

Citra digital yang digunakan sebagai media penyembunyian data adalah citra bitmap (*.bmp) 24 bit serta penyisipan file berupa text menggunakan metode MELSBR dengan pengujian PSNR.

II. METODE PENELITIAN

1. Identifikasi Masalah
2. Penetapan Tujuan
3. Pengumpulan beberapa data dari berbagai sumber yang ada
4. Analisa Sistem
5. Perancangan Sistem
6. Implementasi
7. Pengujian PSNR
8. Kesimpulan dan Saran

III. HASIL DAN PEMBAHASAN

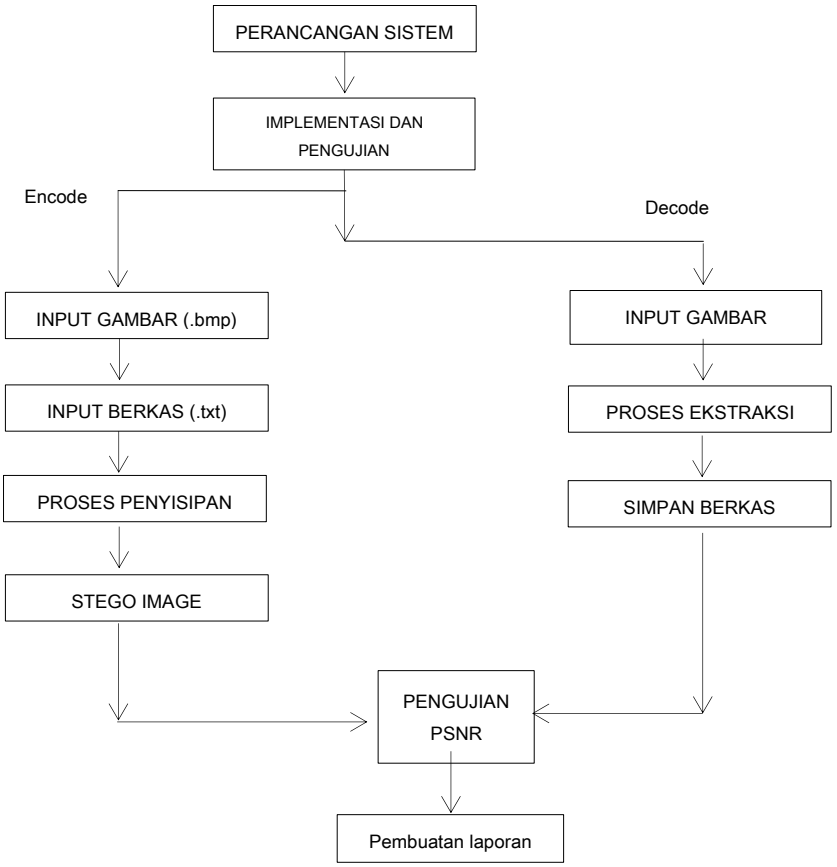
3.1. Perancangan Sistem

Perancangan sistem aplikasi dalam penelitian ini dapat disajikan pada Gambar 2 yaitu langkah-langkah penelitian menggunakan *metode waterfall*. Berikut ini akan dijelaskan tentang pengimplementasian dari analisis dan perancangan yang telah dilakukan terhadap aplikasi steganografi ini. Implementasi penelitian ini yaitu menerjemahkan teori teknik *steganografi* menggunakan metode *MELSBR* dalam melakukan proses penyisipan berkas dengan format *file* (.txt) sebagai berkas yang akan disisipi, media gambar dengan format *file* (.bmp) sebagai media penampung dan melakukan ekstraksi berkas dengan memasukan *stego image* hasil proses penyisipan untuk mendapatkan kembali berkas yang disisipi kedalam bentuk coding program Matlab 2016.

3.1.1. Proses Encode

Dalam tahap ini disajikan pada diagram alir gambar 3. Tahapan dalam proses encode yaitu :

1. Input file gambar
   Dengan memasukkan file gambar berupa (.bmp)
2. Verifikasi file gambar
   Setalah dilakukan penginputan file akan dproses verifikasi gambar (.bmp)
3. Input berkas file
   Memasukkan berkas yang akan disisipkan berupa file text
4. Verifikasi berkas file
   Melakukan verifikasi berkas file text yang sudah di inputkan
5. Proses Steganografi
   Proses Steganografi diproses dengan menggunakan metode MELSBR
6. Selesai



Gambar 2 : Diagram Alir Perancangan sistem

3.1.2. Proses Decode

Sedangkan tahap proses ini dapat disajikan pada gambar 4 yaitu diagram alir proses decode. Adapun tahapannya sebagai berikut :

1. Input file gambar

   Memasukkan file gambar yang berupa stego image yang sudah disisipkan file text tadi yang sudah tersimpan dengan format (.bmp)

2. Verifikasi file gambar

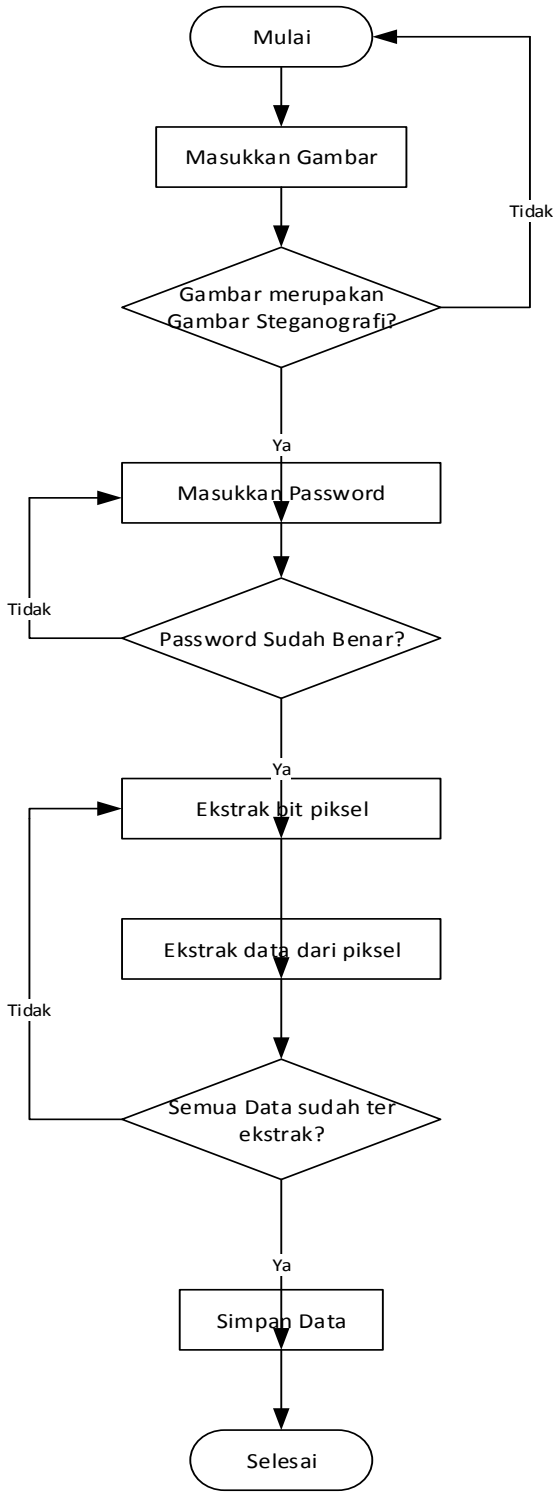
   Dilakukan proses verifikasi gambar harus berformat (.bmp) dalam penyimpanannya

3. Proses Steganografi

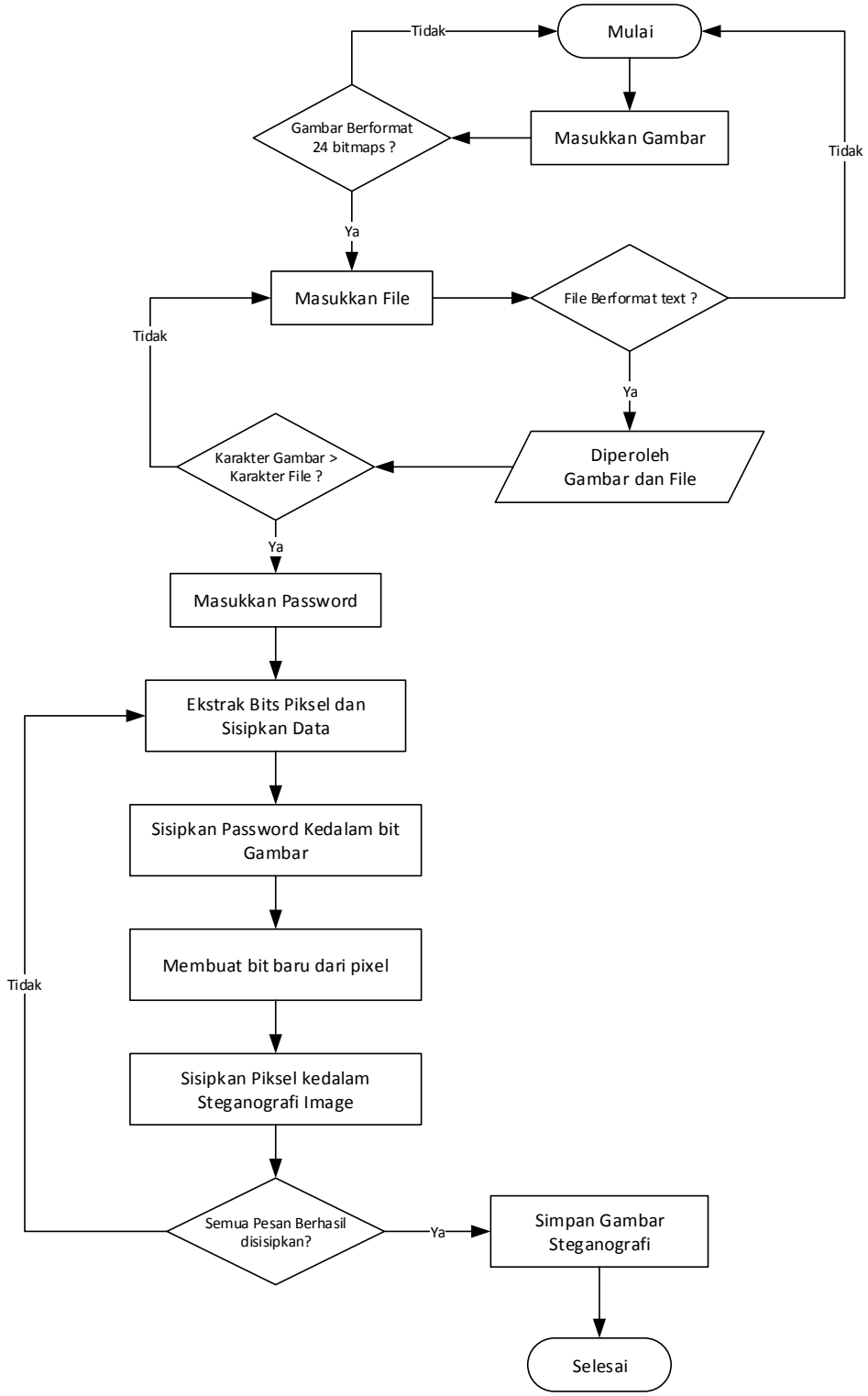
   Proses ini merupakan pengembalian berkas file text dengan menggunakan teknik steganografi metode MELSBR

4. Selesai

   Penyembunyian pesan berhasil disembunyikan sehingga keluaran dari proses ini adal berkas berformat text.

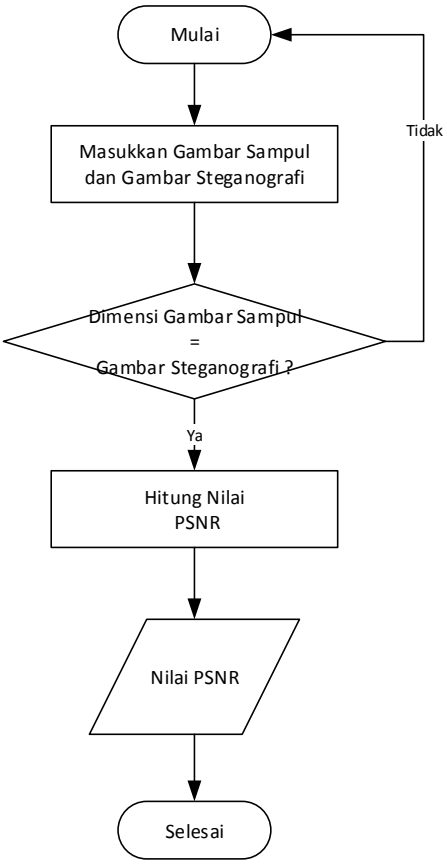


Gambar 3 : Diagram alir Encode



Gambar 4 : Diagram alir Decode

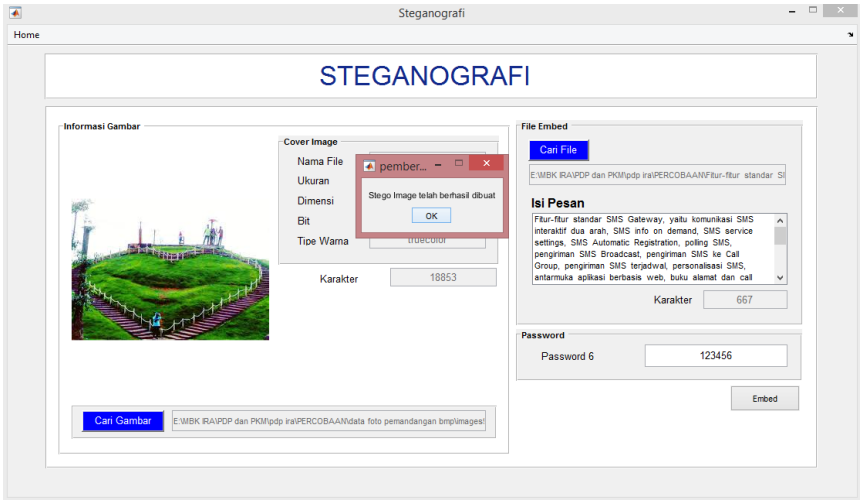
3.1.3. Proses Pengujian



Gambar 5 : Diagram alir pengujian PSNR

3.2. Implementasi dan Pengujian

Proses implementasi penelitian ini, berisi tampilan hasil dari penerapan sistem aplikasi yang telah dirancang dengan menerjemahkan teknik steganografi dengan menggunakan metode MELSBR dalam peyisipan berkas file text dan pengembalian berkas. Adapun tampilan aplikasi yang telah dibuat dengan menggunakan bahasa pemograman Matlab 2016 yaitu dapat disajikan pada gambar 6 dengan proses *decode* dan gambar 7 dengan proses *encode.*



Gambar 6 : Proses Encode

Pada Gambar 6 proses encode ini, menunjukkan bagaimana cara menggunakan encoding dengan memasukkan gambar citra asli serta input file text dengan menggunakan pasword 6 karakter sesuai pengguna untuk menverifikasi gambar asli sudah tersisipkan apa belum kemudian dilakukan proses mengklik tombol embeding untuk mengetahui berhasli tidaknya proses stego imagenya.

Gambar 7 : Proses Encode

Sedangkan gambar 3 yaitu proses decode memperlihatkan bagaimana cara penggunaan decoding sehingga diperoleh hasli ekstraksi yang terverifikasi dan kemudian dari

hasil pengujiannya menggunakan parameter PSNR dengan membandingkan citra asli dengan stego image sehingga akan diketahui kualitas distorsi citranya.

3.3. Pembahasan

Tabel 1 : Perbandingan gambar cover image dengan stego image yang sudah disisipkan file text.

No.	Cover Image	Stego Image
1	 Index4.bmp	 Pengujian 1.bmp
2	 Index.bmp	 Pengujan 3.bmp
3	 Index7.bmp	 Percobaan 5.bmp

Dari hasil Tabel 1 Diperlihatkan citra asli dengan citra yang sudah disisipkan file berkas text, ternyata secara kasat mata tidak mengalami perbedaan yang mencolok dan bisa dikatakan hampir mirip dengan citra aslinya. Oleh karena itu untuk mengetahui perbandingannya antara citra asli dengan citra yang sudah disisipkan oleh berkas file text. Maka perlu dilakukan perbandingan pengujian dengan menggunakan parameter PSNR untuk mengetahuii kualitas distorsi citra hasil dari penyisipan file text tersebut. Berikut disajikan tabel 2. nilai pengujian hasil PSNR dari citra asli dengan citra yang sudah disisipkan oleh file text dengan penyembunyiaan data citra bitmap (*bmp) 24 bit dengan menggunakan metode MELSBR dengan gambar cover image dan stego image yang disajikan pada Tabel 1.

Tabel 2. Nilai pengujian PSNR dari citra asli dan stego image.

Cover image	File Pesan	Ukuran	Stego image	Ukuran	Rata-rata PSNR
Index4.bmp	Fitur-fitur standar SMS Gateway.txt	152234 byte	Pengujian 1.bmp	152150 byte	95,7525
Index.bmp	Fitur-fitur standar SMS Gateway.txt	150834 byte	Pengujan 3.bmp	150750 byte	95,5871
Index7.bmp	Fitur-fitur standar SMS Gateway.txt	150942 byte	Percobaan 5.bmp	150858 byte	95.1174

Diperlihatkan pada Tabel 2 yaitu file cover image beserta nama file pesan yang berupa txt dengan file yang sama namun dengan membedakan cover image dan ukuran yang berbeda. Hasil dari stego image yang telah disisipkan pesan file text di atas dengan format hasil stego image berupa (.bmp) dengan menghasilkan ukran yang tidak jauh berbeda dengan cover image. Rerata PSNR bernilai besar dan hampir sama yaitu 95db.

IV. KESIMPULAN

Penyembunyian pesan dengan media penamoung berupa gambar bitmap dengan penyisipan file text dengan menngunakan Metode MELSBR ternyata dapat disimpulkan metode yang digunakan oleh peneliti ini baik. Sistem implememtasi dari hasil perbandingan citra asli dengan stego image tidak mengalami perbedaan yang mencolok sehingga penyembunyian pesan tersebut dapat dikatakan berhasil dengan baik karena tidak terlihat adanya pesan rahasia yang tersembunyi. Dalam pengujian menggunakan parameter PSNR ternyata dapat disimpulkan bahwa semakin besar nilai PSNR, maka hasli pemrosesan citra semakin bagus atau semakin mendekati citra aslinya.

DAFTAR PUSTAKA

[1]. A Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Biometric Inspired Digital Image Steganography," in *15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ecbs 2008)*, 2008, pp. 159-168.

[2]. Andono, P. N, dkk. (Pengolahan Citra Digital). Semarang. Penerbit Andi. Hal 77.

[3]. Gan, M. D.2003."*Chameleon Image Steganography*".Tehnical Paper, hal 1-8.

[4]. Hmood, Ali K. 2010. "*On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates"*. International Journal of the Physical Sciences, Vol. 5(7), hal 1054-1062.