STMIK Amik Riau

**SATIN – Sains dan Teknologi Informasi**

**journal homepage : http://jurnal.stmik-amik-riau.ac.id**

# Aplikasi Steganografi pada Media Citra Digital Menggunakan Metode Least Significant Bit (LSB)

Yusuf Anshori
*Universitas Tadulako*
*anshoriyusuf80@gmail.com*

A.Y. Erwin Dodu
*Universitas Tadulako*
*ayerwin.dodu@gmail.com*

Megawati Purwaningsih
*Universitas Tadulako*
*mega06.mp@gmail.com*

## Abstrak

*Untuk dapat melakukan proses pengiriman pesan biasanya dibutuhkan suatu cara untuk menjaga keamanan pesan tersebut, agar pesan tidak mudah di ketahui oleh orang lain. Salah satu teknik untuk menyembunyikan pesan yaitu steganografi. Steganografi merupakan ilmu dan seni yang mempelajari teknik dan cara penyembunyian pesan rahasia kedalam suatu media sedemikian rupa sehingga pihak ketiga tidak dapat melihat dan menyadari keberadaan pesan rahasia tersebut. Pada penelitian ini membahas mengenai bagaimana metode least significant bit dapat digunakan untuk menyembunyikan pesan ke dalam file citra. Untuk jenis pesan yang dapat disembunyikan berupa pesan teks, pesan gambar dan pesan dokumen yang di ekstrak kedalam bentuk rar. Metode LSB mengganti bit-bit data RGB citra yang paling kanan dengan bit-bit data pesan rahasia. Metode penelitian yang digunakan adalah waterfall model. Berdasarkan pengujian yang dilakukan metode LSB dapat digunakan untuk menyembunyikan pesan tanpa membuat perubahan dari segi bentuk maupun ukuran pesan rahasia yang disembunyikan juga dapat diekstrak kembali tanpa mengalami kerusakan.*

*Kata Kunci: Least Sigificant Bit, RGB, Steganografi, waterfall model, file citra*

## Abstract

*To be able to process the sending of messages, it usually requires a way to maintain the security of the message, so that the message is not easily known by others. One technique for hiding messages is steganography. Steganography is the science and art that studies the techniques and ways of hiding secret messages into a media in such a way that a third party cannot see and be aware of the existence of the secret message. This study discusses how the least significant bit method can be used to hide messages into image files. For types of messages that can be hidden in the form of text messages, picture messages and messages extracted documents into rar form. The LSB method replaces the rightmost bits of image RGB data with secret message data bits. The research method used is the waterfall model. Based on the tests carried out the LSB method can be used to hide messages without making changes in terms of the size and form of hidden messages that can also be extracted again without damage.*

*Keywords: Least Sigificant Bit, RGB, Steganografi, waterfall model, image file*

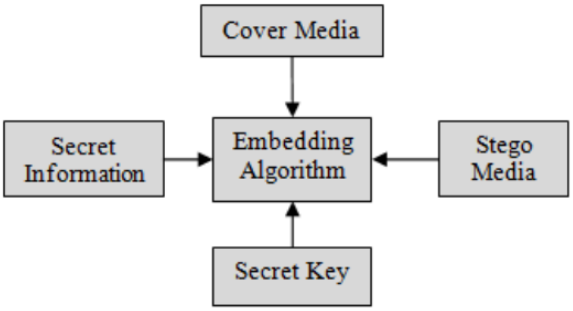
## 1. Pendahuluan

Pesatnya pertumbuhan penggunaan internet melalui kapasitas *bandwidth* yang tinggi dan perangkat keras komputer berbiaya rendah telah mendorong pertumbuhan steganografi yang eksplosif (Goel, Rana, & Kaur, 2013). Steganografi adalah teknik yang digunakan untuk menyembunyikan keberadaan data dalam berbagai format seperti teks, gambar, audio, atau video (Siddiqui & Goswami, 2017). Ketika informasi yang dikirimkan dianggap sensitif, sangat penting untuk melindunginya dari pihak yang tidak berwenang. Oleh karena itu, sistem keamanan yang kuat harus dilibatkan. Steganografi adalah salah satu dari sistem keamanan yang dapat digunakan untuk mengamankan

transmisi antar pengirim dan penerima (Beroual & Al-Shaikhli, 2018).

Steganografi sering disamakan dengan kriptologi karena keduanya mirip dalam cara keduanya digunakan untuk melindungi informasi penting (Chandramouli & Memon, 2003). Perbedaan keduanya adalah Steganografi melibatkan penyembunyian informasi sehingga nampaknya tidak informasi yang disembunyikan sama sekali. Jika seseorang atau beberapa orang melihat objek yang informasinya disembunyikan di dalamnya, dia tidak akan tahu bahwa ada informasi tersembunyi, oleh karena itu orang tersebut tidak akan berusaha melakukan dekripsi informasi. Steganografi pada dasarnya mengeksploitasi persepsi manusia. Indra manusia tidak terlatih untuk mencari file yang terdapat informasi tersembunyi di dalamnya (Bandyopadhyay, Bhattacharyya, Ganguly, Mukherjee, & Das, 2008).

Teks, gambar digital, audio digital dan video digital telah menjadi objek utama untuk menyembunyikan data. Berikut ini adalah beberapa istilah umum yang perlu untuk diketahui mengenai sistem steganografi yang juga diilustrasikan pada Gambar 1 (Choudry & Wanjari, 2015; Tripathi, Singh, & Singh, 2016).




**Gambar 1. Proses Steganografi**

*Cover Media*: Media dimana informasi rahasia ditanam sedemikian rupa sehingga sulit untuk dideteksi keberadaannya.

*Stego-Media*: Media yang diperoleh setelah menanamkan informasi rahasia.

*Secret data*: Data atau informasi yang akan disembunyikan di *cover media*.

*Steganalysis*: Proses mendeteksi keberadaan data rahasia di *cover media*.

Ada banyak teknik steganografi, steganografi gambar adalah teknik yang banyak digunakan dibandingkan dengan yang lain karena kesederhanaannya dan memiliki cara termudah untuk menyembunyikan data dalam gambar (Al-Husainy, 2011). Pendekatan sederhana untuk menanamkan informasi dalam gambar adalah menggunakan metode *Least Significant Bits* (LSB). Kekuatan metode *Least Significant Bits* (LSB) adalah kesederhanaan perhitungan dan sejumlah besar data dapat disembunyikan dalam gambar aslinya dengan tingkat visual yang tinggi (Siddiqui & Goswami, 2017).

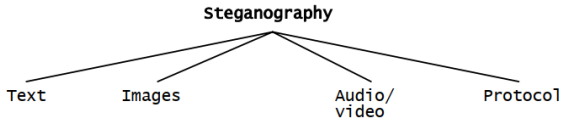
Menurut Poornima & Iswarya, metode *Least Significant Bits* (LSB) adalah teknik umum dalam mengenkripsi dan mendekripsi informasi rahasia. Metode LSB didasarkan pada mengubah bit-bit redundan dengan tingkat kepentingan paling rendah dengan bit-bit informasi rahasia. Tujuan LSB adalah untuk mengirimkan informasi rahasia ke penerima tanpa membuat curiga penyusup bahwa pesan sedang disampaikan (Poornima & Iswarya, 2013).

LSB menggunakan format file BMP 24-bit cocok dan efisien karena gambar BMP sudah memiliki kualitas yang bagus dan resolusi tinggi sehingga informasi yang disembunyikan tidak dapat dideteksi mata manusia.

Berdasarkan uraian diatas, maka penelitian ini bertujuan untuk membuat suatu aplikasi steganografi pada citra digital menggunakan metode metode *Least Significant Bits* (LSB) yang dapat diterapkan untuk kebutuhan keamanan data.

## 2. Tinjauan Pustaka

Hampir semua format file digital dapat digunakan untuk steganografi, tetapi format yang lebih cocok adalah format dengan tingkat redundansi yang tinggi. Gambar 2 menunjukkan empat kategori utama format file yang dapat digunakan untuk steganografi (Morkel, Eloff, & Olivier, 2005).




**Gambar 2. Kategori Steganografi**

Steganografi teks menggunakan file digital tidak sering digunakan karena file teks memiliki jumlah redundan yang sangat kecil. Gambar adalah objek paling populer yang digunakan untuk steganografi. Di domain digital, terdapat banyak format file gambar yang berbeda, sebagian besar untuk aplikasi tertentu. Untuk format file gambar yang berbeda ini, terdapat berbagai algoritma steganografi.

Untuk menyembunyikan informasi dalam file audio, dapat menggunakan teknik serupa untuk file gambar. Satu teknik berbeda untuk audio steganografi adalah masking, yang mengeksploitasi sifat-sifat telinga manusia untuk menyembunyikan informasi tanpa disadari.

Istilah protokol steganografi mengacu pada teknik menanamkan (*embedding*) informasi dalam pesan dan protokol kendali jaringan yang digunakan dalam transmisi jaringan (Ahsan & Kundur, 2002).

Mengingat semakin banyaknya gambar digital, terutama di internet dengan tingkat redundansi yang berlebihan dalam representasi digital dari suatu gambar, maka penelitian ini akan fokus dalam

menyembunyikan informasi pada gambar (citra digital) dengan referensi dari beberapa penelitian sebelumnya mengenai steganografi pada gambar (citra digital).

Prabowo, Hidayatno, & Christiyono menerapkan *discrete cosine transform* dan *chaos theory* untuk membuat suatu sistem berbasis pengolahan citra yang dapat digunakan untuk melakukan steganografi data rahasia digital (citra, teks, atau suara) pada media penampung citra digital, serta untuk mengetahui kinerja program tersebut dan keandalannya terhadap berbagai operasi manipulasi data. (Prabowo, Hidayatno, & Christiyono, 2012).

Edisuryana, Isnanto, & Somantri dalam penelitiannya mengimplementasikan teknik kriptografi dan steganografi pada citra berformat bitmap dengan menggunakan metode *end of file* (EOF). Metode kriptografi yang digunakan adalah *caesar cipher* dan *zig-zag cipher*. Berdasarkan penggunaan aplikasi, didapatkan hasil bahwa pada tahap enkripsi dengan metode *caesar chiper* perlu diperhatikan karakter pesan dan karakter pengganti spasi agar tidak saling tumpang tindih. Steganografi dengan menggunakan metode *end of file* (EOF) tidak merusak kualitas dari citra asli/citra cover, sehingga citra asli dengan citra stego nampak mirip dan sulit dibedakan secara kasat mata. Steganografi dengan menggunakan metode *end of file* (EOF) mengakibatkan ukuran citra yang disisipi pesan mengalami penambahan ukuran tinggi (Height) dan ukuran berkasnya (Edisuryana, Isnanto, & Somantri, 2013).

Marhaeni merancang aplikasi steganografi pada media citra digital terkompresi *joint photographic experts group* (jpeg) menggunakan aplikasi *stephy*. Dari hasil penelitian menunjukan bahwa menyembunyikan file di dalam gambar dapat membantu meningkatkan keamanan data (Marhaeni, 2017).

Siregar, Ramadhani, & Siregar mengimplementasikan steganografi pada citra digital menggunakan algoritma *diversity*. Dari hasil uji coba, diketahui bahwa dengan algoritma *diversity*, penyisipan dan ekstraksi pesan dapat dilakukan dengan baik (Siregar, Ramadhani, & Siregar, 2018).

Nurfauzan, Hidayat, & Saida menganalisis steganografi ganda pada citra digital menggunakan metode *discrete wavelet transform* dan *singular value decomposition* dengan penyisipan *spread spectrum image steganography*. Metode *spread spectrum image steganography* digunakan untuk metode penyisipan pertama pada domain spasial, sedangkan pada penyisipan kedua digunakan metode *discrete wavelet transform* untuk mentransformasi cover citra kedua ke domain frekuensi dan pesan disisipkan dengan memodifikasi singular value dengan menggunakan metode *singular value decomposition*. Hasil penelitian menunjukan stego-file yang dihasilkan memiliki *imperceptibility* dan *robustness* yang cukup baik. Hal ini diukur berdasarkan nilai PSNR dan SNR pada kedua proses penyisipan, SSIM pada penyisipan kedua dan BER pada saat proses ekstraksi (Nurfauzan, Hidayat, & Saida, 2018).

Menyembunyikan informasi di dalam gambar adalah teknik yang populer saat ini. Pendekatan sederhana untuk menanamkan (*embedding*) informasi dalam gambar *cover* adalah dengan menggunakan metode *Least Significant Bits* (LSB) (Nosrati, Karimi, & Hariri, 2011).

Selain sederhana, metode *Least Significant Bits* (LSB) juga mudah diimplementasikan. Media penampungnya berupa gambar digital karena jumlahnya yang besar di internet. Kehandalan penggunaan citra dibandingkan dengan media lain adalah kualitas citra yang telah disisipi pesan rahasia tidak berbeda jauh dengan kualitas citra aslinya (Yenni, 2012).

Metode *Least Significant Bits* (LSB) bekerja pada bit yang terendah dari suatu deretan bit data. Penggunaan metode *Least Significant Bits* (LSB) ini dengan menyisipkannya pada bit rendah atau bit yang paling kanan pada data pixel yang menyusun gambar tersebut. Seperti di ketahui untuk file bitmap 24 bit di setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (*byte*) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111 (Mesran, 2012).

Dalam penelitian ini akan dibangun aplikasi steganografi pada media citra digital menggunakan metode *Least Significant Bits* (LSB), gambar berformat BMP (*bitmap*) 24-bit digunakan sebagai media untuk penyembunyian pesan, serta file pesan yang akan disembunyikan berupa teks ataupun dokumen (pdf, *word, excel, txt*) dalam betuk *file* rar sehingga informasi yang akan disampaikan terhadap orang lain tidak mudah diketahui oleh orang-orang yang tidak mempunyai hak untuk mengaksesnya, serta tanpa menimbulkan rasa keingintahuan seseorang terhadap informasi tersebut.

## 3. Metode Penelitian

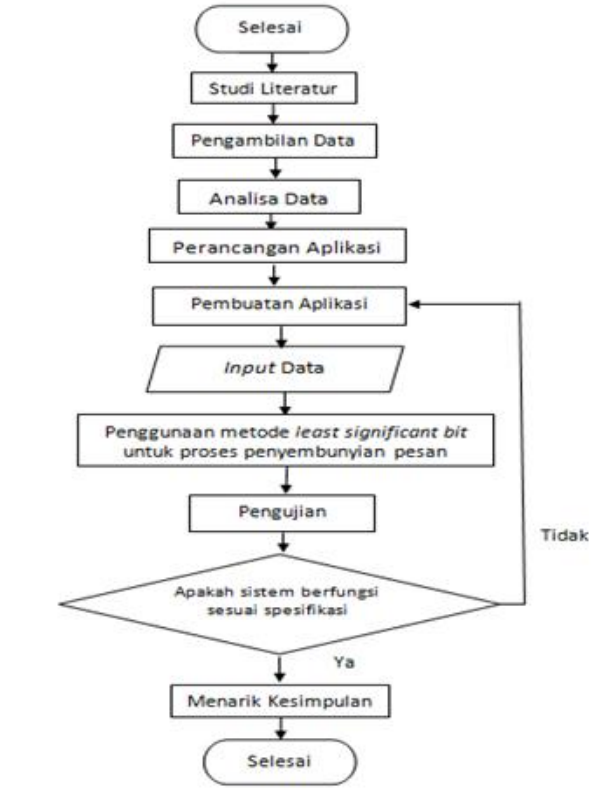
Penelitian ini menggunakan bentuk penelitian studi literatur dan metode penelitian eksperimen murni. Peneliti melakukan kajian mengenai permasalahan yang hendak dipecahkan serta mendefinisikan masalah dengan melakukan eksperimen. Selain itu pencarian referensi dan informasi yang diperlukan dari buku-buku dan artikel-artikel di internet juga dilakukan. Referensi dan informasi tersebut merupakan dasar pembuatan aplikasi.

Pendekatan yang digunakan pada penelitian ini dalam melakukan penggalian data dan informasi yaitu metode UML (*Unified Modelling Language*). Adapun beberapa jenis UML yang digunakan antara lain *Use*

*Case Diagram, Activity Diagram, Sequential Diagram* dan *Flowchart*.

Metode pengembangan sistem yang digunakan dalam penelitian ini yaitu Model *Waterfall*. Model ini merupakan sebuah pendekatan terhadap pengembangan perangkat lunak yang sistematik, dengan beberapa tahapan, yaitu: *requirements definition, system and software design, implementation and unit testing, integration and system testing, operation and maintenance*.

Tahapan penelitian digambarkan pada Gambar 3 di bawah ini.




**Gambar 3. Flowchart Tahapan Penelitian**

Terdapat beberapa tahapan yang dilakukan dalam membangun aplikasi steganografi menggunakan metode *Least Significant Bits (LSB)* yaitu dengan proses *embed* dan proses ekstrak pesan sebagai berikut.

A. Proses *embed* pesan

Pada proses *embed* pesan akan dilakukan beberapa tahapan yaitu:

1. *Input* gambar

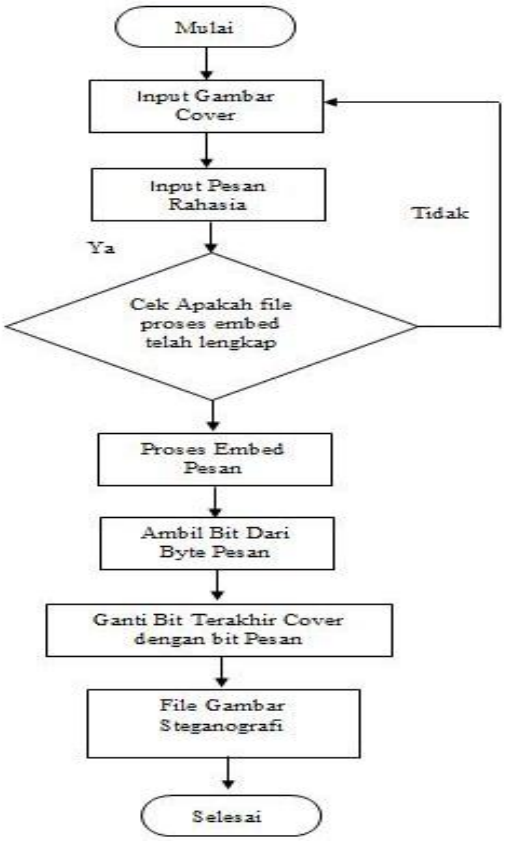
   *Input* gambar yang akan digunakan sebagai media untuk menyembunyikan pesan, baik berupa pesan teks, pesan gambar, maupun pesan dokumen. Jenis citra yang dapat digunakan yaitu citra berformat bitmap dengan kedalam piksel 24 bit.
2. *Input* pesan

   Pengguna memilih jenis pesan yang akan disisipkan atau disembunyikan ke dalam citra yang telah dipilih sebelumnya.
3. Proses *Embed*

   Setelah pengguna memilih gambar (media pesan) dan jenis pesan yang akan disembunyikan akan dilakukan proses *embed*, dimana sistem akan membaca RGB *file* citra dan mengubah dari bilangan desimal ke bentuk bilangan biner.
4. Proses Penyisipan

   Proses penyisipan pesan ke dalam gambar (*file* citra) secara berurutan menggunakan metode *least significant bit.* Sebagai contoh citra penampung yang telah diubah menjadi kode biner adalah (**10011000)** (**10111000) (00110111) (01001110)** dan data rahasia yang akan disisipkan sebelumnya telah diubah ke kode biner adalah **1100** maka hasil steganografi menggunakan metode LSB menghasilkan **1001100<u>1</u> 1011100<u>1</u> 0011011<u>0</u> 0100111<u>0</u>.** Pengambilan bit pesan dimasukkan atau ditukar kedalam bit RGB pada gambar, sehingga dihasilkan *file* citra steganografi yang telah terisi pesan rahasia.

Tahapan-tahapan diatas diatas dapat digambarkan pada diagram alir yang terdapat pada Gambar 4.

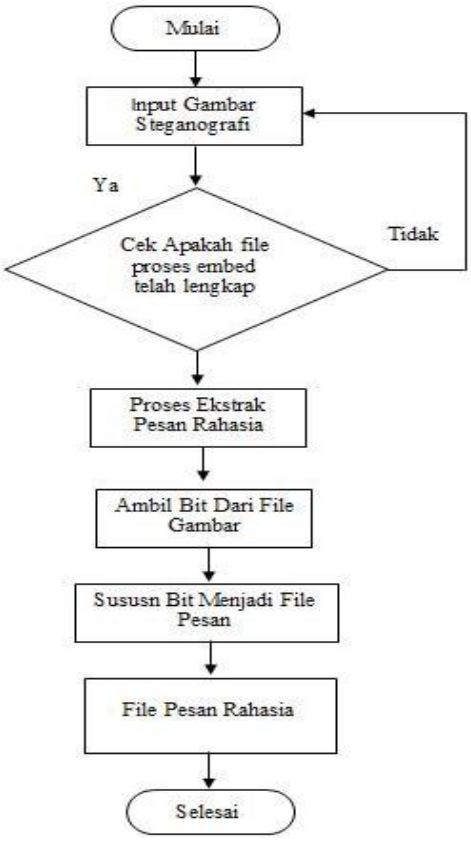



**Gambar 4. Flowchart Embed Pesan Rahasia**

B. Proses ekstrak pesan

Pada proses ekstrak pesan akan dilakukan beberapa tahapan yaitu:

1. Proses *input*
   Pada proses input pengguna memilih *file* steganografi yang telah tersimpan untuk mengekstrak pesan yang terdapat pada citra bitmap.
2. Proses ekstrak
   Proses ekstrak dilakukan untuk mengungkap pesan yang disisipkan kedalam *file* citra. Proses awalnya adalah membaca RGB *file* citra, dan mengubah RGB *File* citra kedalam format biner. Proses selanjutnya sistem membangkitkan bit bit atau koefisien yang berada pda *file* citra atau gambar steganografi. Setelah diperoleh koefisisen atau bit-bit yang mengandung pesan proses ekstraksi akan berjalan dan menghitung jumlah *byte* pesan yang tersembunyi pada gambar steganografi.
3. Proses Penyusunan bit
   Setelah diperoleh koefisisen atau bit-bit yang mengandung pesan, proses ekstraksi akan berjalan dan menghitung jumlah byte pesan yang tersembunyi pada gambar steganografi, kemudian sistem akan menyusun kembali pesan yang telah disisipakan pada *file* gambar steganografi. Data biner yang diperoleh dari file gambar steganografi adalah **10011001 10111001 00110110 01001110,** sehingga bit pesan rahasia disusun kembali menjadi **1100.** Penerima pesan dapat mengetahui isi pesan yang ada pada gambar steganografi. Tahapan-tahapan proses ekstrak pesan diatas dapat dilihat pada Gambar 5.




**Gambar 5. Flowchart Ekstraksi Pesan Rahasia**

## 4. Hasil dan Pembahasan

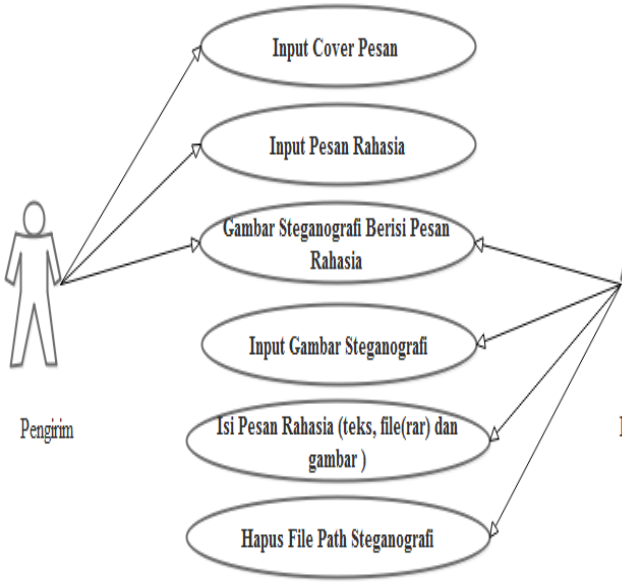
A. Analisa Sistem

a) *Usecase Diagram*

*Usecase diagram* menggambarkan hubungan yang terjadi antara aktor dengan aktivitas yang ada pada sistem. Pengguna atau user pengirim memilih citra yang akan digunakan sebagai media penyembunyian pesan, kemudian user memilih jenis pesan yang akan disembunyikan (teks, gambar, dan file dokumen) ke dalam citra, dan kemudian menekan tombol embed pesan. Sistem akan langsung memproses penyembunyian pesan kedalam citra. Hasil dari proses embed adalah citra yang telah disisipi pesan rahasia.

Sedangkan *user* penerima adalah pengguna yang menerima pesan steganografi. User penerima memilih gambar steganografi yang berisi pesan rahasia (teks, gambar, dan file dokumen), kemudian user penerima menekan tombol ekstrak pesan maka pesan rahasia yang tersembunyi dalam citra akan ditampilkan dan dapat dsimpan ditempat yang sesuai dengan keinginan penerima. Untuk mencegah pihak ketiga mengetahui pesan rahasia yang tersimpan di dalam gambar

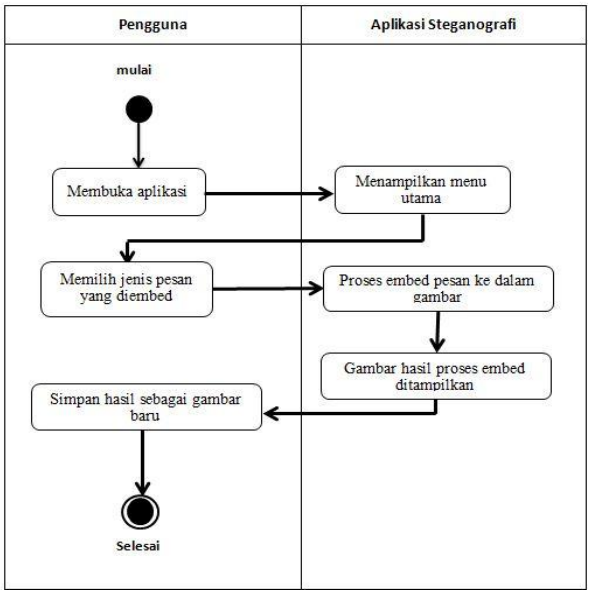
steganografi, maka *user* penerima dapat menghapus file path gambar steganografi yang tersimpan di dalam PC penerima pesan. Gambar 10 menunjukkan *usecase diagram* pada aplikasi yang telah dibuat.



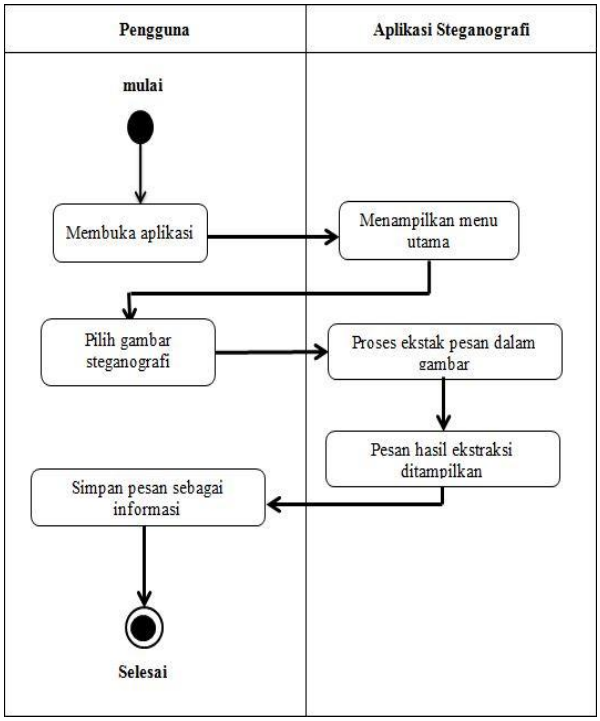

**Gambar 6. *Use Case Diagram* Aplikasi Steganografi**

b) *Activity Diagram* Proses Embed dan Ekstrak Aplikasi Steganografi

*Activity diagram* pada palikasi steganografi ini digunakan untuk menggambarkan dan mendeskripsikan alur logika dari rangkaian proses yang berjalan pada sistem (aplikasi). *Activity diagram* pada aplikasi ini menggambarkan aktivitas-aktivitas yang terjadi dalam sistem untuk menyisipkan pesan ke dalam gambar, dimulai dari *user* memasukkan gambar sampai pada tahap akhir yaitu user menyimpan gambar hasil dari proses steganografi sebagai *file* gambar baru yang berisi pesan rahasia. Begitu pula tahapan yang akan dilakukan untuk mengambil atau melihat pesan rahasia yang ada di dalam citra sama dengan tahapan penyisipan pesan hanya saja proses yang dipilih adalah ekstrak pesan. Keseluruhan aktivitas yang terjadi di dalam sistem aplikasi, dikelompokkan ke dalam 2 bagian, yaitu bagian pengguna dan bagian sistem. Activity Diagram embed dan activity diagram ekstrak pesan dapat dilihat pada Gambar 11 dan Gambar 12.




**Gambar 7. *Activity Diagram Proses* Embed Aplikasi Steganografi**




**Gambar 8. *Activity Diagram* Proses Ekstrak Aplikasi Steganografi**

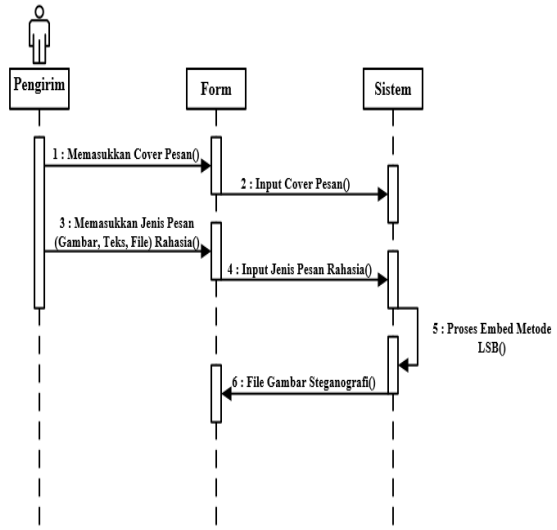
c) *Sequencial Diagram*

Sequencial diagram pada aplikasi steganografi menjelaskan dua proses, yaitu proses *embedding* pesan rahasia dan proses ekstraksi pesan rahasia.

(1) *Sequencial diagram* proses *embed* pesan

Sequencial diagram proses embed pada aplikasi steganografi menggambarkan urutan alur

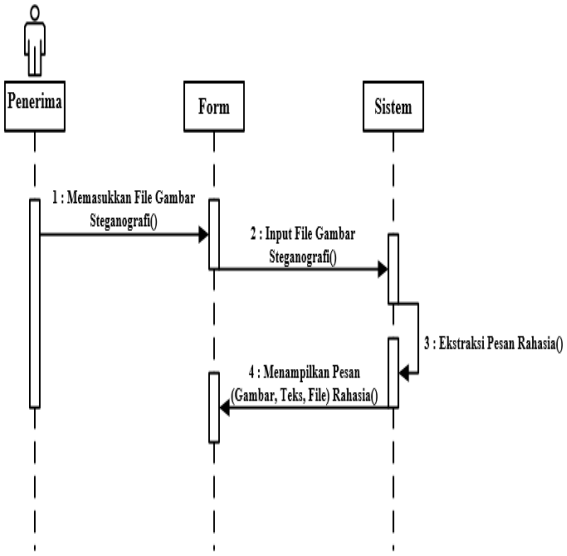
pengirim pesan untuk melakukan proses embed pesan rahasia. Pertama pengirim memasukkan cover pesan sesuai dengan pilihan pengirim, kemudian memasukkan jenis pesan rahasia yang ingin disembunyikan ke dalam form aplikasi steganografi. Setelah cover dan pesan rahasia dimasukkan, sistem akan melakukan proses embedding pesan rahasia menggunakan metode LSB dan menampilkan file gambar steganografi yang berisi pesan rahasia. Gambar 13 Menunjukkan sequencial diagram proses embed aplikasi steganografi.




**Gambar 9. *Sequential Diagram* Proses Embed Aplikasi Steganografi**

(2) *Sequencial diagram* proses ekstrak pesan

Tahapan proses ekstrak pada aplikasi steganografi dapat dilihat pada sequencial diagram proses ekstrak pesan rahasia. Pertama-tama penerima pesan memasukkan file gambar steganografi ke dalam *form*, kemudian sistem akan melakukan proses ekstraksi pesan rahasia secara otomatis, setelah proses ekstrak selesai sistem akan menampilkan isi pesan rahasia yang disembunyikan di dalam gambar steganografi. Gambar 14 menunjukkan *sequencial* proses ekstraksi pesan rahasia pada aplikasi steganografi.




**Gambar 10. *Sequential Diagram* Proses Ekstraksi Aplikasi Steganografi**

B. Implementasi Sistem

a) Implementasi *Hardware* dan *Software*

Implementasi hardware rancang bangun aplikasi steganografi pada media citra digital menggunakan metode Least Significant Bit. Menggunakan Acer Aspire dengan spesifikasi processor intel inside, memori RAM 2 Gigabyte, dan hardisk 320 Gigabyte.

Untuk implementasi *software* digunakan bahasa pemrograman C# dengan tools Microsoft Visual Basic.Net 2012 sebagai media pembuatan dan perancangan aplikasi steganografi pada media citra digital menggunakan metode *Least Significant Bit.*

b) Implementasi Antarmuka Sistem

Implementasi antar muka aplikasi steganografi pada media citra digital menggunakan metode *Least Significant Bit* yaitu sebagai berikut.

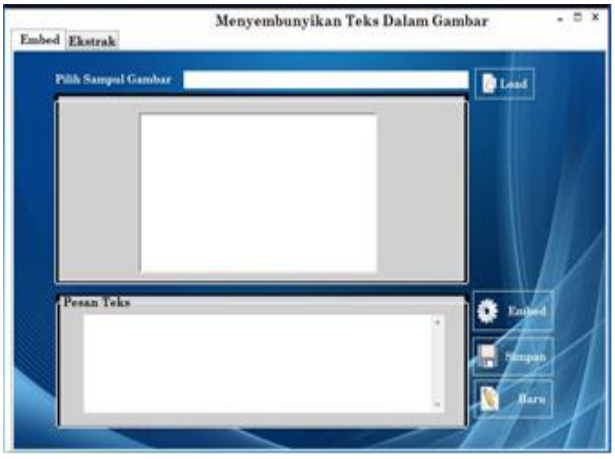
1. *Form* Menu Utama

Pada *form* menu utama terdapat beberapa pilihan menu yaitu menu untuk menyembunyikan pesan teks dalam gambar, menu menyembunyikan pesan gambar dalam gambar, dan menu menyembunyikan dokumen (*file*) dalam gambar.


**Gambar 11. *Form* Menu Utama**

2. *Form* menyembunyikan pesan teks di dalam gambar

Pada *form* menyembunyikan pesan teks dalam gambar terdapat dua proses yaitu *embed* dan ekstrak. Pada proses *embed* terdiri dari empat button yaitu button cari, *embed*, simpan, dan hapus. Sebelum melakukan proses *embed* tekan button cari untuk memilih gambar yang akan digunakan sebagai media untuk menyembunyikan pesan teks, kemudian ketik pesan pada textbox. Setelah selesai mengetik pesan tekan button *embed* untuk melakukan proses penyisipan pesan teks ke dalam gambar, sehingga output yang dihasilkan adalah gambar steganografi. Untuk menyimpan gambar pilih button simpan. Sedangkan pada proses ekstrak pesan tampilan dan tahapan yang dilakukan sama dengan tahapan *embed* pesan yang m*embed*akan hanya pada button ekstrak.

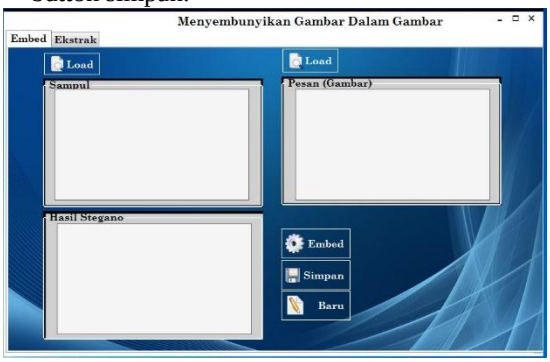



**Gambar 12. *Form* Menyembunyikan Pesan Teks di dalam Gambar**

3. *Form* menyembunyikan pesan gambar di dalam gambar

Pada form menyembunyikan pesan gambar di dalam gambar ada dua proses yang dilakukan yaitu proses *embed* dan proses ekstrak. Dalam form proses *embed* terdapat lima button yaitu button *load* sampul untuk memilih *cover* gambar sebgai media penyembunyian pesan, *load* pesan digunakan untuk memilih pesan gambar yang akan disembunyikan ke dalam *cover*, *embed* untuk proses penyisipan pesan, simpan untuk menyimpan *file* steganografi dan hapus untuk menghapus gambar-gambar yang ada di *picturebox*.

Sebelum melakukan proses *embed* terlebih dahulu kita memilih sampul dan pesan gambar yang akan disisipkan kemudian pilih button *embed* untuk melakukan proses penyisipan pesan. Setelah proses selesai output yang dihasilkan adalah *file* gambar steganografi, kemudian gambar disimpan pada folder yang diinginkan. Sedangkan untuk melakukan proses ekstrak terlebih dahulu tekan button telusuri gambar untuk mengambil gambar steganografi yang disimpan sebelumnya kemudian tekan button ekstrak gambar, jika ingin menyimpan pesan gambar yang telah diekstrak maka tekan button simpan.



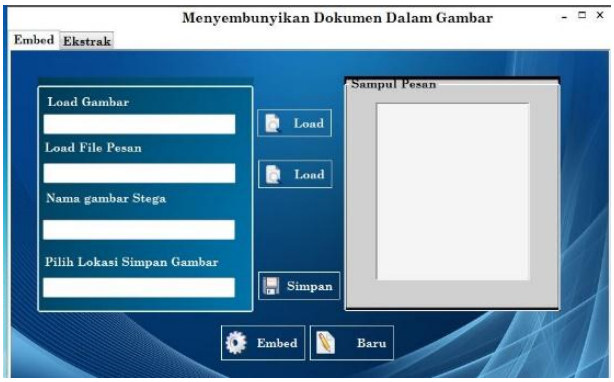

**Gambar 13. *Form* Menyembunyikan Pesan Gambar di dalam Gambar**

4. *Form* menyembunyikan pesan dokumen (*rar*) didalam gambar

Pada form menyembunyikan pesan gambar di dalam gambar ada dua proses yang dilakukan yaitu proses *embed* dan proses ekstrak. Dalam form proses *embed* terdapat lima button yaitu button *load* sampul untuk memilih *cover* gambar sebgai media penyembunyian pesan, *load* pesan digunakan untuk memilih pesan gambar yang akan disembunyikan ke dalam *cover*, *embed* untuk proses penyisipan pesan, simpan untuk menyimpan *file* steganografi dan hapus untuk menghapus gambar-gambar yang ada di *picturebox*.

Sebelum melakukan proses *embed* terlebih dahulu kita memilih sampul dan pesan gambar

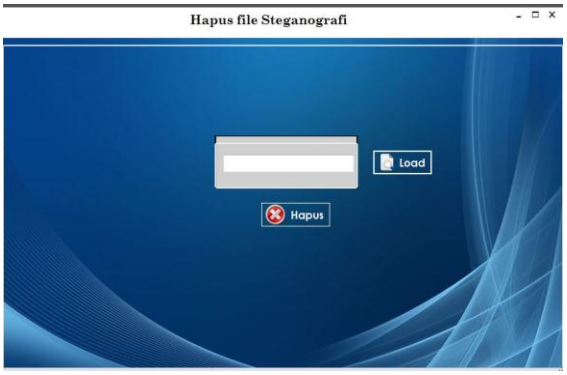
yang akan disisipkan kemudian pilih button *embed* untuk melakukan proses penyisipan pesan. Setelah proses selesai output yang dihasilkan adalah *file* gambar steganografi, kemudian gambar disimpan pada folder yang diinginkan. Sedangkan untuk melakukan proses ekstrak terlebih dahulu tekan button telusuri gambar untuk mengambil gambar steganografi yang disimpan sebelumnya kemudian tekan button ekstrak gambar, jika ingin menyimpan pesan gambar yang telah diekstrak maka tekan button simpan.




**Gambar 14. *Form* Menyembunyikan Pesan Dokumen (*File*) di dalam Gambar**

5. *Form* hapus file pesan steganografi

Pada form hapus file pesan steganografi digunakan untuk menghapus file asli steganografi yang dimiliki oleh penerima pesan, hal ini dilakukan agar orang lain tidak mencoba untuk mengekstrak kembali isi pesan yang ada didalm file steganografi. Sebelum melakukan proses hapus *file*, pengguna terlebih dahulu memilih file steganografi yang ingin dihapus menggunakan *button* load yang ada pada form tersebut. Setelah file ditemukan kemudian tekan *button* delete untuk menghapus file steganografi, maka file yang tersimpan didalam folder penyimpanan akan langsung terhapus.




**Gambar 15. *Form* Hapus File Pesan Steganografi**

## 5. Simpulan

Berdasarkan pengujian sistem yang telah dilakukan, maka dapat disimpulkan ke dalam beberapa hal yaitu:

1. Metode *least significant bit* telah berhasil digunakan untuk menyembunyikan pesan teks, pesan gambar dan pesan dokumen (*rar*) ke dalam citra *bitmap*
2. Proses penyisipan pesan dapat dilakukan dengan tiga jenis pesan rahasia yaitu pesan berupa teks, gambar, dan juga dokumen dalam bentuk *file* rar.
3. Pada steganografi gambar dalam gambar hanya dapat menyisipkan pesan gambar yang memiliki ukuran yang sama dengan *cover* pesan.
4. Aplikasi steganografi hanya dapat mengembed dan mengekstrak gambar yang memiliki kedalaman piksel 24 bit.
5. Metode *least significant bit* dapat menyembunyikan pesan dengan cara mengganti bit paling kanan *cover* dengan bit-bit pesan rahasia.
6. Pada pengujian ketahanan isi pesan menggunakan jaringan dengan media email, pesan berhasil diekstrak kembali tanpa mengurangi isi pesan.

## 6. Referensi

Ahsan, K., & Kundur, D. (2002). Practical Data Hiding in TCP / IP (Vol. 2). Proc. Workshop on Multimedia Security at ACM Multimedia.

Al-Husainy, M. (2011). A New Image Steganography Based on Decimal-Digits Representation. *Computer and Information Science*, *4*(6), p38. https://doi.org/10.5539/cis.v4n6p38

Bandyopadhyay, S. K., Bhattacharyya, D., Ganguly, D., Mukherjee, S., & Das, P. (2008). A Tutorial Review on Steganography. *International Conference on Contemporary Computing*, *101*, 105–114.

Beroual, A., & Al-Shaikhli, I. F. (2018). A Review of Steganographic Methods and Techniques. *International Journal on Perceptive and Cognitive Computing (IJPCC)*, *4*(1). http://dx.doi.org/10.31436/ijpcc.v4i1.56

Chandramouli, R., & Memon, N. D. (2003). Steganography capacity: a steganalysis perspective. In *Security and Watermarking of Multimedia Contents V* (Vol. 5020, pp. 173–178). International Society for Optics and Photonics. https://doi.org/10.1117/12.479732

Choudry, K. N., & Wanjari, A. (2015). A Survey Paper on Video Steganography. *International Journal of Computer Science and Information Technologies*, *6*(3), 2335–2338.

Edisuryana, M., Isnanto, R. R., & Somantri, M. (2013). Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode End Of File. *Transient*, *2*(3), 734–742.

Goel, S., Rana, A., & Kaur, M. (2013). A Review of Comparison Techniques of Image Steganography. *Global Journal of Computer Science and*

*Technology*. Retrieved from https://computerresearch.org/index.php/computer/article/view/407

Marhaeni, M. (2017). Perancangan Aplikasi Steganografi Pada Media Citra Digital Terkompresi JoinT PHOTOGRAPHIC EXPERTS GROUP (JPEG). *Incomtech*, *6*(1). Retrieved from https://ejournal.istn.ac.id/index.php/incomtech/article/view/24

Mesran, M. (2012). Aplikasi Pengamanan Data Teks Pada Citra Bitmap Dengan Menerapkan Metode Least Significant Bit (LSB). *Pelita Informatika: Informasi Dan Informatika*, *2*(1). Retrieved from https://ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/111

Morkel, T., Eloff, J. H., & Olivier, M. S. (2005). An overview of image steganography. *ISSA*, 1–11.

Nosrati, M., Karimi, R., & Hariri, M. (2011). An introduction to steganography methods. *World Applied Programming*, *1*(3), 191–195.

Nurfauzan, R. A., Hidayat, B., & Saida, S. (2018). Analysis Of Double Digital Image Steganography Using Discrete Wavelet Transform And Singular Value Decomposition Method With Spread Spectrum Image Steganography Insertion. *E-Proceeding of Engineering*, *5*(1), 299.

Poornima, R., & Iswarya, R. . (2013). An Overview of Digital Image Steganography. *International Journal of Computer Science & Engineering Survey (IJCSES)*, *4*(1). http://dx.doi.org/10.5121/ijcses.2013.4102

Prabowo, A., Hidayatno, A., & Christiyono, Y. (2012). *Penyembunyian Data Rahasia Pada Citra Digital Berbasis Chaos Dan Discrete Cosine Transform* (other). Diponegoro University. Retrieved from http://eprints.undip.ac.id/32526/

Siddiqui, B., & Goswami, S. (2017). A Survey On Image Steganography Using Lsb Substitution Technique. *International Research Journal of Engineering and Technology (IRJET)*, *4*(5). Retrieved from www.irjet.net

Siregar, D., Ramadhani, R., & Siregar, Y. S. (2018). Implementasi Steganografi Menggunakan Algoritma Diversity Pada Citra Digital. *Jurnal Teknologi Dan Ilmu Komputer Prima (JUTIKOMP)*, *1*(1), 102–114.

Tripathi, D., Singh, Y. K., & Singh, R. (2016). A Review on Digital Image Steganography with its Techniques and Model. *IJSART*, *2*(4).

Yenni, H. (2012). Steganografi LSB 3 Bit pada Gambar Digital dengan Key Terenkripsi Vigenere Chiper. *SATIN - Sains Dan Teknologi Informasi*, *1*(2), 10–14. https://doi.org/10.33372/stn.v1i2.319