

Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganografi Menggunakan Metode *Least Significant Bit*

Achmad Ardiansyah¹, Mepa Kurniasih²

^{1,2}Fakultas Teknologi Informasi, Universitas Budi Luhur Jakarta

¹ahd.ardiansyah@gmail.com, ²mepa.kurnia@gmail.com

INTISARI

Pesan merupakan hasil dari pengolahan data menjadi bentuk yang lebih berguna bagi yang menerimanya yang menggambarkan suatu fakta yang digunakan sebagai alat bantu untuk pengambilan suatu keputusan. Sangat pentingnya isi pesan yang menyebabkan pesan hanya boleh diakses oleh orang-orang tertentu. Pesan yang merupakan aset bernilai seharusnya dilindungi agar aman. Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Pesan yang dapat disembunyikan berupa teks, gambar, suara, dan video.

Melindungi pesan yang dirahasiakan dari orang yang tidak berhak salah satunya adalah teknik steganografi yang dapat menyembunyikan data rahasia. Teknik steganografi menggunakan metode *Least Significant Bit (LSB)* untuk memodifikasi bit-bit yang termasuk bit *LSB* pada setiap byte warna pada sebuah pixel citra digital. Bit-bit *LSB* ini akan dimodifikasi dengan menggantikan setiap *LSB* yang ada dengan bit-bit informasi lain yang ingin disembunyikan. Dengan adanya citra digital kita bisa memanfaatkan untuk menyisipkan pesan pada citra digital tersebut. Hasil penelitian menunjukkan bahwa semakin besar ukuran pixel citra dan jumlah karakter, maka akan semakin lama proses penyisipan dan ekstraksinya. Dengan stego-image yang diperoleh secara citra digital memiliki tampilan hampir sama sehingga tidak terlihat oleh sistem penglihatan manusia.

Kata Kunci – Citra Digital, *Least Significant Bit (LSB)*, Steganografi, Pesan

ABSTRACT

Message is the result of processing data into a form that is more useful for those who receive it which describes a fact that is used as a tool for making a decision. The importance of the contents of messages causes messages to only be accessed by certain people. Messages that are valuable assets should be protected to be safe. Steganography is the art and science of writing hidden messages or hiding messages in a way so that in addition to the sender and the recipient, no one knows or realizes that there is a secret message. Messages that can be hidden are in the form of text, images, sounds, and videos.

Protecting confidential messages from unauthorized people is one of the Steganography Techniques that can hide confidential data. The steganography technique uses the *LSB (Least Significant Bit)* method to modify the bits including the *LSB* bit on each color byte in a digital image pixel. These *LSB* bits will be modified by replacing each existing *LSB* with other bits of information that you want to hide. With the presence of digital images we can use to insert messages in the digital image. The results of the study show that the larger the pixel size of the image and the number of characters, the longer the insertion process and its extraction will be. With stego-image obtained by digital imagery it has almost the same appearance so it is not visible to the human visual system.

Keywords — Digital Image, *Least Significant Bit (LSB)*, Steganography, Message

I. PENDAHULUAN

Keamanan suatu pesan pada era digital ini makin vital peranannya dalam berbagai aspek kehidupan, terutama untuk suatu pesan yang memiliki nilai lebih dibandingkan dengan pesan yang lain. Pesan merupakan hasil dari pengolahan data menjadi bentuk yang lebih berguna bagi yang menerimanya yang menggambarkan suatu fakta yang digunakan

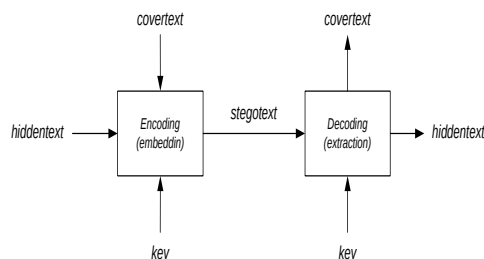
sebagai alat bantu untuk pengambilan suatu keputusan. Sangat pentingnya isi pesan yang menyebabkan pesan hanya boleh diakses oleh orang-orang tertentu. Pesan yang merupakan aset bernilai seharusnya dilindungi agar aman. Berdasarkan uraian diatas, maka rumusan masalah dalam penelitian ini tersebut yaitu "Bagaimana cara membuat aplikasi untuk penyembunyian pesan pada citra digital

menggunakan metode Least Significant Bit (LSB) ?" Penelitian ini akan membahas proses untuk menyembunyikan pesan dengan steganografi menggunakan LSB. Dengan rumusan masalah tersebut, maka penelitian ini bertujuan untuk membuat sebuah aplikasi steganografi untuk menyimpan pesan rahasia menggunakan metode Least Significant Bit dan memberikan informasi bagaimana teknik steganografi metode Least Significant Bit (LSB) dapat diterapkan dalam pengamanan citra digital.

II. TINJAUAN PUSTAKA

A. *Steganografi*

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata "steganografi" berasal dari bahasa Yunani *steganos*, yang artinya "tersembunyi atau terselubung", dan *graphein*, "menulis". Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam praktiknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritme yang digunakan.[1]



Gambar 1 : Diagram encoding dan decoding

B. *Citra Digital*

Citra sebagai keluaran suatu sistem perekaman data dapat bersifat optik berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan

pada suatu pita magnetik. Citra digital merupakan suatu larik dua dimensi atau suatu matriks yang elemen-elemennya menyatakan tingkat keabuan dari elemen gambar. Jadi informasi yang terkandung bersifat diskret. Citra digital tidak selalu merupakan hasil langsung data rekaman suatu sistem. Kadang-kadang hasil rekaman data bersifat kontinu seperti gambar pada monitor televisi, foto sinar-X, dan lain sebagainya. Dengan demikian untuk mendapatkan suatu citra digital diperlukan suatu proses konversi, sehingga citra tersebut selanjutnya dapat diproses dengan komputer. Pengolahan Citra merupakan proses pengolahan dan analisis citra yang banyak melibatkan persepsi visual. Proses ini mempunyai ciri data masukan dan informasi keluaran yang berbentuk citra. Istilah pengolahan citra digital secara umum didefinisikan sebagai pemrosesan citra dua dimensi dengan komputer. Dalam definisi yang lebih luas, pengolahan citra digital juga mencakup semua data dua dimensi. Citra digital adalah barisan bilangan nyata maupun kompleks yang diwakili oleh bit-bit tertentu. [5]

C. *Metode LSB (Least Significant Bit)*

Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, 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. Dengan demikian, pada setiap pixel berkas bitmap 24 bit kita dapat menyisipkan 3 bit data.[1]

Pada citra 24 bit, setiap piksel terdiri dari 3 byte yang merepresentasikan warna red (merah), green (hijau), dan blue (biru). Sebagai contoh dalam gambar yang berukuran 600 x 500 piksel, satu piksel berukuran 3 byte (sehingga bisa disisipkan 3 bit pada setiap piksel), maka dapat disisipkan pesan sebanyak $600 \times 500 \times 3 = 900000$ bit, atau dengan kata lain $900000 / 8 = 112500$ byte pesan yang dapat disisipkan (1 byte = 8 bit). Gambar di bawah ini adalah contoh gambar yang akan disisipi informasi. Gambar ini menggunakan format pewarnaan grayscale, artinya tiap pixel

dari gambar ini direpresentasikan dengan nilai sepanjang 8 bit [6].



Gambar 2. Nilai sepanjang 8 bit

Misalkan data berupa text “secret” hendak disisipkan dalam gambar ini. Jika direpresentasikan ke dalam binary kata “secret” ini menjadi

TABEL I.
TEXT KE DALAM BINARY

character	ASCII value (decimal)	hexadecimal	Binary
s	115	73	01110011
e	101	65	01100101
c	99	63	01100011
r	114	72	01110010
e	99	63	01100011
t	116	74	01110100

Sesuai dengan namanya, LSB artinya bit yang tidak significant / tidak mempunyai pengaruh yang besar, maka metode ini mengganti nilai bit ke-8 gambar Lena untuk menyisipkan data.

Media (gambar Lena.jpg)

00000000	00000001	00000001	00000001	00000000	00000000	00000001	00000001
00000000	00000001	00000001	00000000	00000000	00000001	00000000	00000001
00000000	00000001	00000001	00000000	00000000	00000000	00000001	00000001
00000000	00000001	00000011	00000011	00000010	00000010	00000011	00000010
00000000	00000001	00000011	00000010	00000010	00000010	00000011	00000011
00000000	00000001	00000011	00000011	00000010	00000011	00000010	00000010

Data yang ingin disisipkan (kata “secret”)

0	1	1	1	0	0	1	1
0	1	1	0	0	1	0	1
0	1	1	0	0	0	1	1
0	1	1	1	0	0	1	0
0	1	1	0	0	0	1	1
0	1	1	1	0	1	0	0

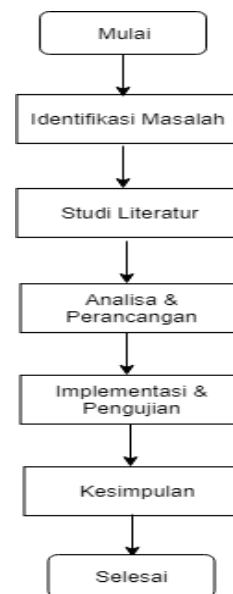
HASIL AKHIR (STEGO):

00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011

Setelah dikonstruksi ulang dari representasi binernya, gambar Lena yang telah disisipi informasi akan menjadi Gambar yang telah disisipi informasi nyaris tidak memiliki perbedaan dengan gambar aslinya, karena yang diubah adalah bit paling belakang dari representasi biner gambar tersebut sehingga perubahannya tidak nampak oleh mata [6].

III. METODOLOGI PENELITIAN.

Metodelogi yang digunakan pada penulisan ini penulis menggunakan beberapa metode untuk memudahkan penulis dalam pembuatan aplikasi. Berikut ini metode penulisan tersebut :



Gambar 3. metodologi penelitian

A. Identifikasi Masalah

Pada tahap ini proses yang dilakukan adalah mengidentifikasi masalah tentang bagaimana membangun suatu aplikasi steganografi untuk menyembunyikan pesan rahasia dan dapat melindungi keamanan datanya yang disisipkan pada gambar dengan menggunakan metode *Least Significant Bit* (LSB) sehingga kerahasiaan datanya tetap terjamin aman dan secara kasak mata tidak terjadi perubahan pada gambar tersebut meskipun telah disisipi data yang rahasia.

Proses penyisipan pesan pada citra tentu memiliki beberapa permasalahan termasuk untuk mengecek apakah pesan sudah benar dan tepat disisipkan dalam citra, hasil penyisipan citra juga tidak membuat kecurigaan pada pihak lain.

B. Study Literatur

Pada tahap ini akan dilakukan dengan mempelajari literatur-literatur yang dapat membantu dalam aplikasi steganografi untuk menyembunyikan pesan rahasia. Literatur tersebut pemahaman tentang bagaimana konsep yang ada pada steganografi. Literatur tersebut bersumber dari buku, artikel, dan situs-situs di internet adalah untuk memperdalam permasalahan yang ada untuk keamanan data menggunakan steganografi.

C. Analisa & Perancangan

Pada tahap ini melakukan analisis kebutuhan dengan mengidentifikasi kebutuhan dari aplikasi menggunakan metode *Least Significant Bit* (LSB). Untuk menganalisa bagaimana cara kerja algoritma *Least Significant Bit* (LSB) yang terdiri dari proses *embed* sampai proses penyisipan dan proses *extract* sampai proses output yang sesuai. Langkah dalam perancangan aplikasi yaitu perancangan diagram alir aplikasi tersebut, bahasa pemrograman yang digunakan, library yang digunakan. Penelitian bersifat implementatif perancangan yang artinya aplikasi yang dirancang akan diimplementasikan.

D. Implementasi & Pengujian

Pada tahap ini dilakukan pengujian terhadap aplikasi yang telah dibuat. Proses implementasi dilakukan untuk membuat model aplikasi yang telah dirancang pada perancangan aplikasi menjadi sebuah aplikasi yang dapat memenuhi kebutuhan dan menyelesaikan permasalahan pada latar belakang. Pengujian berfokus pada fungsionalitas keamanan datanya. Hal ini dilakukan untuk mengetahui kinerja dan kekurangan sistem, untuk menguji apakah aplikasi yang telah dibuat sudah dapat memenuhi kebutuhan yang telah diidentifikasi sebelumnya. Hasil dari pengujian dapat dijadikan acuan untuk tahap perbaikan aplikasi selanjutnya.

E. Kesimpulan

Pada tahap akhir dilakukan pengambilan kesimpulan dan saran. Kesimpulan diambil dari hasil pengujian terhadap aplikasi yang

telah dibangun. Saran dimaksudkan untuk memperbaiki kekurangan yang terjadi dan menyempurnakan penulisan serta pengembangan penelitian yang lebih lanjut.

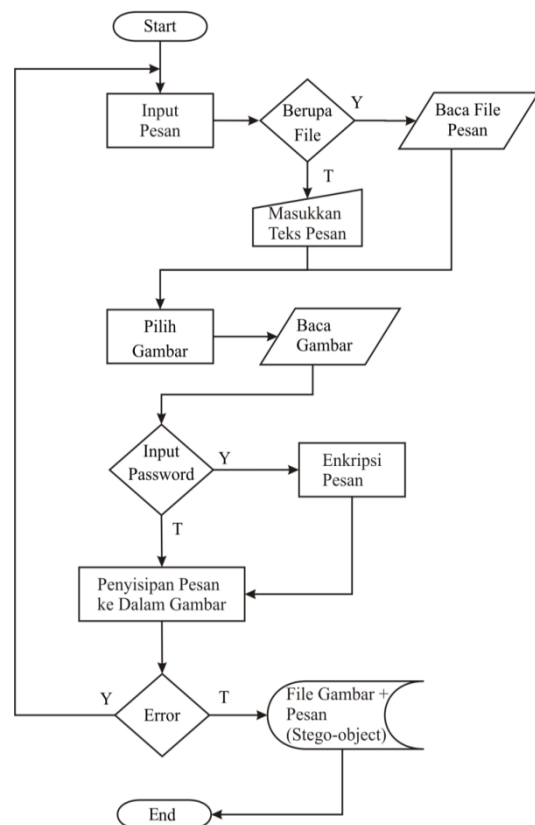
IV. HASIL DAN PEMBAHASAN

A. Flowchart

Untuk mengetahui proses *embed* dan *extract*, Berikut ini menggambarkan beberapa urutan – urutan proses yang harus dilalui, digambarkan dalam bentuk *flowchart* sebagai penjelasan.

Flowchart Embed

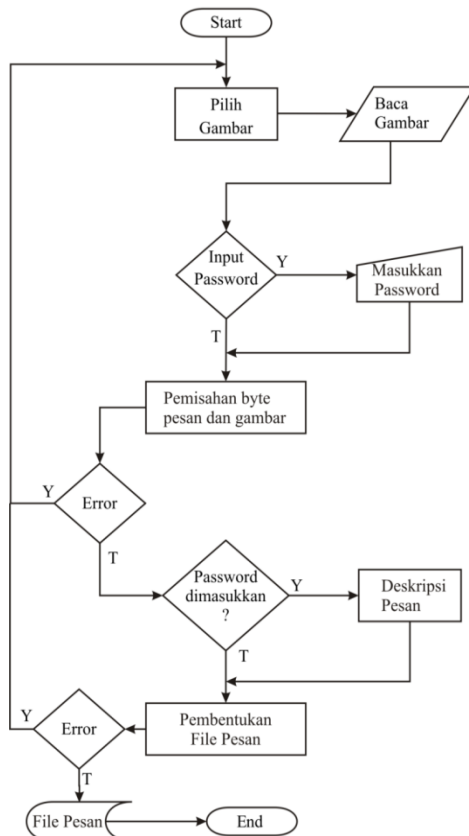
Berikut ini adalah *flowchart embed*, sebelum penyisipan file dalam *image*. Urutan proses yang akan dilalui pada *embed* digambarkan dengan *flowchart* pada gambar berikut ini:



Gambar 4. Flowchart Embed

Flowchart Extract

Berikut ini adalah *flowchart extract*, untuk mengetahui isi pesan pada stego object. Urutan proses yang akan dilalui pada *extract* digambarkan dengan *flowchart* pada gambar berikut ini:



Gambar 5. Flowchart extract

B. Cara Pengoperasian Aplikasi

Berikut ini akan diberikan penjelasan dan gambar mengenai tampilan-tampilan yang ada pada program aplikasi steganografi ini:

Tampilan Layar Proses Loading

Sebelum menampilkan form menu utama, terlebih dahulu menampilkan proses *loading* seperti tampilan pada gambar :



Gambar 6 : Tampilan Layar proses loading

Tampilan Layar Embed

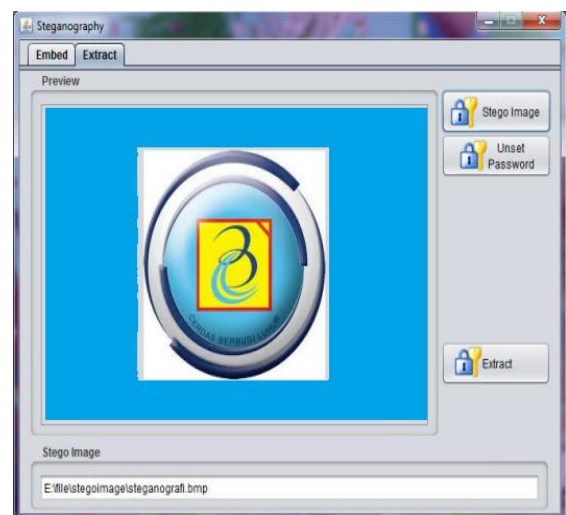
Pada tampilan layar ini berfungsi untuk menyisipkan pesan file ke dalam *image*. Berikut ini tampilan layar *embed* :



Gambar 7. Tampilan Layar embed

Tampilan Layar Extract

Pada tampilan layar ini berfungsi untuk mengekstrak image yang disisipi file pesan, supaya pesana bisa diketahui penerima. Berikut ini tampilan layar *extract* :



Gambar 8. Tampilan Layar extract

C. Pengujian Program

Pengujian program untuk memastikan keberhasilan jalannya aplikasi tersebut. Pengujian tersebut untuk mengetahui *performance*, *embed* pesan dengan citra digital, supaya proses aplikasi berjalan dengan baik. Berikut ini pengujian program tersebut :

Pengujian Embed Pesan

Untuk Penyembunyian Pesan Rahasia pada Citra Digital dengan Teknik Steganografi Menggunakan Metode *Least Significant Bit* (LSB) di perlukan pengujian *embed* pesan untuk mengetahui menyembunyikan pesan berupa text, gambar, audio dan video. Berikut ini tabel pengujian *embed* pesan:

TABEL II.
HASIL PENGUJIAN *EMBED* PESAN

Citra Asli			Embed Pesan		Status	Stego Image
Nama Citra	Pixel Citra	Size (KB)	Nama File	Size (KB)		
Image 1.jpg	3000 x 2000	496	File 1.mov	1,420	Berhasil	Image 1.bmp
Image 2.jpg	2000 x 1000	628	File 2.mp3	600	Berhasil	Image 2.bmp
Image 3.gif	472 x 364	4,72	File 3.docx	18	Berhasil	Image 3.bmp
Image 4.gif	400 x 344	24,8	File 4.docx	750	Gagal	-
Image 5.png	300 x 762	1239,04	File 5.pdf	159	Berhasil	Image 5.bmp
Image 6.png	400 x 300	99,8	File 6.txt	5	Berhasil	Image 6.bmp
Image 7.bmp	796 x 573	1331,2	File 7.mp3	600	Gagal	-
Image 8.bmp	600 x 393	38,2	File 8.xlsx	21	Berhasil	Image 8.bmp

Pengujian *Extract* Pesan

Setelah kita melakukan pengujian *embed* pesan, kita akan melakukan pengujian *extract* pesan. Berikut ini tabel pengujian *extract* pesan tersebut:

TABEL III.
HASIL PENGUJIAN *EXTRACT* PESAN

Stego Image		Extract Pesan	
Nama	Size (KB)	Nama File	Size (KB)
Image 1.bmp	17510,4	File 1.mov	1,420
Image 2.bmp	5857,28	File 2.mp3	600
Image 3.bmp	503	File 3.docx	18
Image 5.bmp	2007,04	File 5.pdf	159
Image 6.bmp	351	File 6.txt	5
Image 8.bmp	690	File 8.xlsx	21

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Dari hasil analisis terhadap masalah dan pembahasan yang diuraikan, maka dapat ditarik beberapa kesimpulan antara lain :

- 1) Steganografi algoritma LSB dalam penyembunyian pesan dalam media gambar/citra sesuai dengan baik sehingga tidak terlihat oleh sistem penglihatan manusia.
- 2) Semakin besar ukuran pixel citra dan jumlah karakter, maka akan semakin lama proses penyisipan dan ekstraksinya. Jadi berpengaruh terhadap lamanya waktu proses *embed* dan *extract*.
- 3) Untuk pesan yang disembunyikan bisa menggunakan gambar, video, suara dan file dokumen.
- 4) Pada aplikasi yang dikerjakan terdapat fitur untuk melakukan autentikasi pesan dengan memasukkan password yang diinginkan, supaya komunikasi pertukaran data menjadi rahasia.

B. Saran

Selain menarik beberapa kesimpulan, juga mengajukan beberapa saran yang mungkin bisa dijadikan pertimbangan dalam pengembangan tersebut, antara lain :

- 1) Perlu adanya metode kompresi supaya ukurannya menjadi lebih kecil dan orang lain tidak mengira ternyata ada pesan rahasia pada citra digital.
- 2) Untuk gambar pesan bisa menggunakan dengan format lain seperti jpg, png, gif dan gif.

REFRENSI

- [1] [Online], <http://id.wikipedia.org/wiki/Steganografi>, 2018
- [2] Shelve Nidya Neyman, Lindayati Lindayati, dan Sugi Guritman. Teknik Penyembunyian Data Rahasia pada Berkas Gambar Digital Menggunakan Steganografi Least Significant Bit Variable-Size. Jurnal Ilmu Komputer Agri-Informatika (IPB). Vol 1, No 1, 2012
- [3] Madenda Sarifudin, "Pengolahan Citra dan Vidio Digital", Jakarta, Erlangga, 2015.
- [4] Alim Muadzani, Oky Dwi Nurhayati dan Ike Pertiwi Windasari. Penyisipan Media Teks dan Citra Menggunakan Teknik Steganografi pada Media Pembawa Citra Digital. Jurnal Teknologi dan Sistem Komputer (UNDIP). Vol 4, No 3, 2016
- [5] [Online], <http://elektronika-dasar.web.id/definisi-dan-pengolahan-citra-digital/>, 2018
- [6] [Online], <http://mulinnuha.wordpress.com/2010/01/10/teknik-penyembunyian-informasi-pada-steganografi/>, 2017
- [7] Shikha Sharda and Sumit Budhiraja. Image Steganography: A Review, IJETA. Vol 3, No 1, 2013.
- [8] Priyanka Tirkey, Dipika Kudiya, Neha Dhruw, Deepshikha Markam and Miss Rumi Ghosh. Image Steganography Using LSB Along With IDEA Algorithm. IJECCS . Vol 5, 2016