International Research Journal of Computer Science (IRJCS)
Issue 08, Volume 4 (August 2017)
ISSN: 2393-9842
www.irjcs.com

# Implementation of Steganography in Image Media Using Algorithm LSB (Least Significant Bit)

**Achmad Kodar**
University of Mercu Buana, Indonesia
kodarachmad@gmail.com

**Manuscript History**
Number: **IRJCS/RS/Vol.04/Issue08/AUCS10081**
**DOI: 10.26562/IRJCS.2017.AUCS10081**
Received: 17, July 2017
Final Correction: 26, July 2017
Final Accepted: 29, July 2017
Published: August 2017
Citation: **Achmad, K. (2017). Implementation of Steganography in Image Media Using Algorithm LSB (Least Significant Bit). IRJCS:: International Research Journal of Computer Science, Volume IV, 06-13. doi: 10.26562/IRJCS.2017.AUCS10081**
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India
Copyright: **©2017 This is an open access article distributed under the terms of the Creative Commons Attribution License, Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited**

**Abstract**: The development of Information Technology is very rapid at this time, triggering developments in other fields, one of them in the field of education. Currently, Information Technology is not only viewed as a field of education, but more than that Information Technology began to be developed in order to assist the development of the field of education itself. This is because the development of Information Technology in support of information exchange progress is increasingly dominant in today's society. Information Technology is expected to not only support the development of education alone, but more than that Information Technology is expected to provide solutions on existing educational and information problems. Application of steganography in message insertion will be more valuable that can be used as a positive value tool. In this research will be made system of steganography with LSB (Least Significant Bit) method. With the aim that all the information (message) inserted into the media images, audio and video could not be opened easily by people who have no interest.

**Keywords –**Information Technology, images, audio,steganography, LSB

## I. INTRODUCTION

In the development of information technology, one of the main ideas is security. Some things that must be met when the message is sent to the recipient are confidentiality, integrity, availability, authenticity, and non-repudiation. These five computer security concepts protect messages sent to the receiver by sending the messages delivered safely without less than one bit of data. Confidentiality is a term used to prevent access to information by an individual or an unauthorized system. Integrity in terms of information security means data couled notbe modified without being detected. Availability describes the purpose of the message, where it is required that such information be accessible and available. Authenticity explains that the messages sent are authentic, as well as the sender and receiver are the true parties who actually send the message. Non repudiation is a term to explain a party could not dodge having done a transaction, in this case sending a message. Judging from the above security issues then developed an electronic message security method called steganography (steganography). Steganography is the art of concealment of messages into other messages in such a way that others do not realize there is something in the message conveniently sending a secret message to the image. In this way it will be very difficult to read the invisible message inserted on the image media if the message is not extracted from the image media first, and the message will be stored safely.


© 2014- 17, IRJCS- All Rights Reserved

The method used for concealment of secret messages on the application to be created is by inserting a message into the low bit (LSB - Least Significant Bit) on the pixel data that compiles the image file. This LSB (Least Significant Bit) insertion method is inserting a message by replacing bits to 8, 16 and 24 in the binary representation of the image file with a binary representation of the secret message to be hidden. Thus on every pixel 24 bit BMP image file can be inserted 3 bit message (Masaleno, 2006).

## II. RELATED WORK

Steganography refers to an art of communication, where the art of communication is to insert a message or information to an object. The object can be image, video or sound. If we see it just a normal object without any information or messages in the object. Steganography comes from Greek. Steganos means "hidden or veiled" grape in means "to write". The ancient Greeks claimed to be the inventors of the first steganography, in 440 BC, applied a simple technique to conceal the message in the form of a tattoo on the scalp of a shaved slave, then wait until the hair grows back and the slave is assigned as a messenger to a certain area where the message may not be known by anyone other than the recipient. After arriving at the recipient the hair of the slave is shaved back (shaved) so that the message on the scalp of his head can be read. The purpose of steganography is to conceal or hide the existence of a hidden message or information. In practice, most messages are hidden by making slight changes to other digital data whose contents will not attract the attention of a potential attacker, for example a picture that looks harmless. This change depends on the key (same as in cryptography) and the message to hide. The person receiving the image can then deduce the veiled information by replacing the correct key into the algorithm used. In steganography method this method is very useful when used in the way of computer steganography because many digital file formats that can be used as media to hide messages. Commonly used formats such as:

a. Image format: bitmap (bmp), gif, pcx, jpeg, etc.
b. Audio format: wav, voc, mp3, etc.
c. Other formats: text file, html, pdf, etc.
d. The terminology of steganography has 2 algorithms, one for inserting messages and one for extracting messages. The process of message insertion is to hide messages in the media images, sound or video. And the second algorithm is reading the message, where after the message or information inserted into a media (picture, sound or video) is to read the contents of the information or message

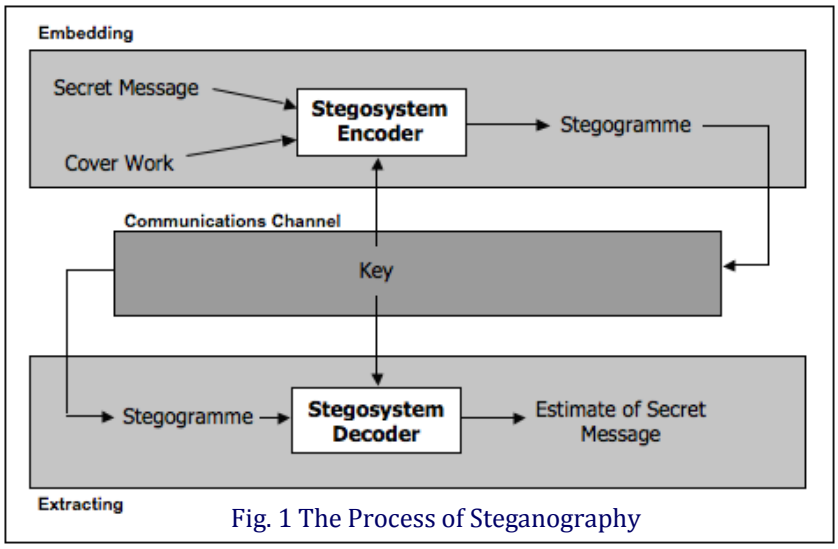


Fig. 1 The Process of Steganography

Stego system encoder is the main part (heart) of a steganography, where the part is the most important in insertion of a message. The message can be inserted into a medium (object) and the object can be received by its recipient without knowing any messages or information in the object. The encoder reads a cover image cm, n, where m and n have the meaning of high an object and the dimension of c. The Stego system decoder allows the stegogramme receiver to get an approximate m of the secret message. This means that the recipient will still get the content of the message within an object without increasing or decreasing the capacity of the object. Steganalysis is a technique used to express the existence of steganography. There is several software that can analyze the use of steganography technique. Some analyze the changes made to the Meta data file. Then others analyze from the file characteristics have been using certain software for steganography.


© 2014- 17, IRJCS- All Rights Reserved

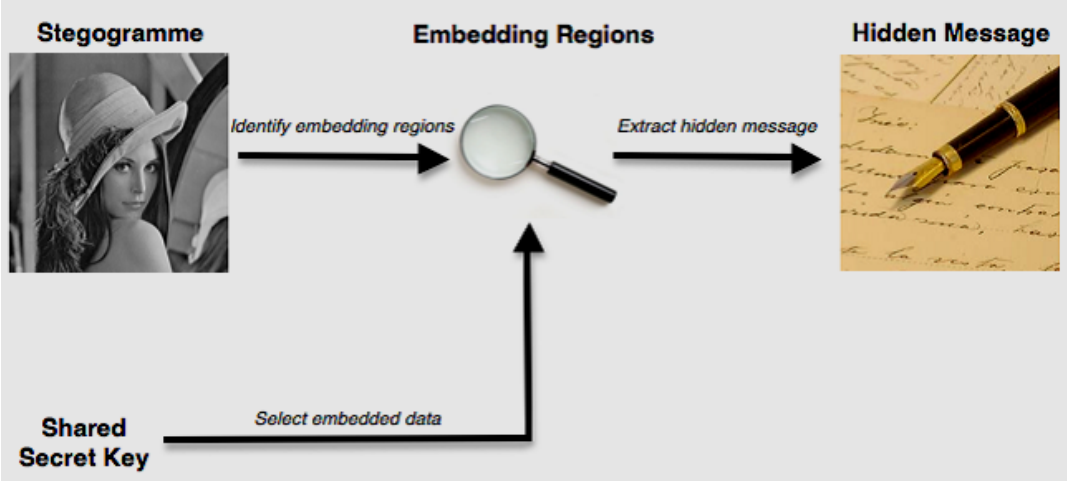


Fig. 2 The general design of a basic stego-system encoder

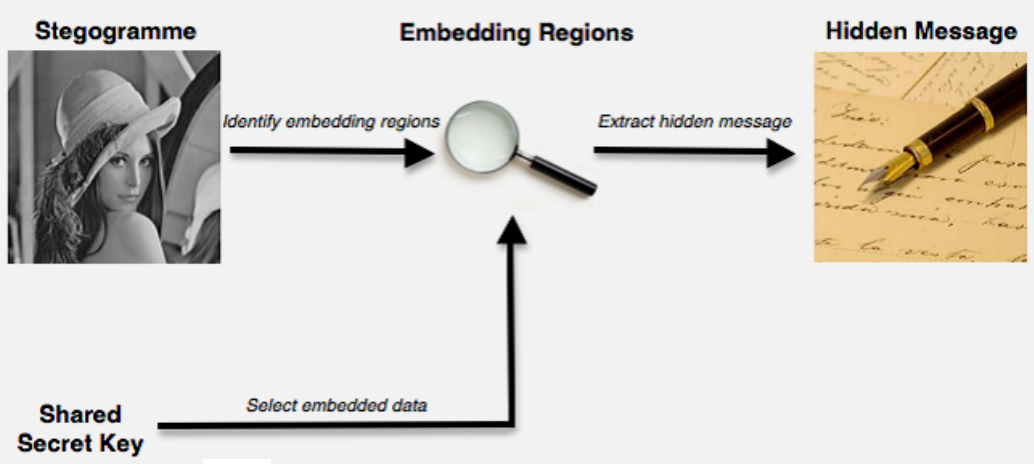


Fig. 3 The general design of a basic stego-system decoder

Some compare the original file, then look for the difference and the pattern used so that in this way not only can the file has experienced steganography process can also know hidden message. But the technique of steganalysis could not be used to find out the hidden message if it turns out the message is cryptographic. So a good way to do steganography is to assume that people will know that there is a hidden message that is done again with cryptography. The selection of cryptography is also not done carelessly and uses a proven efficacy such as 3DES and SHA-1

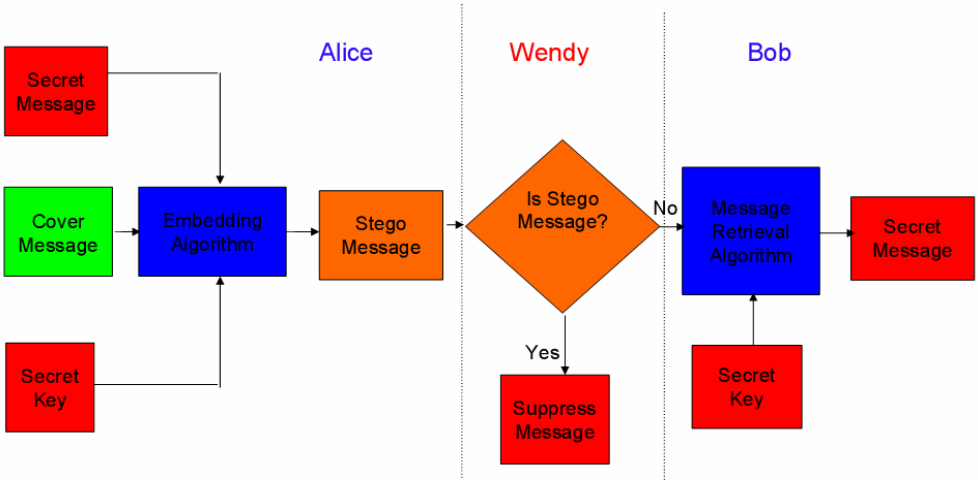


Fig. 4 Steganalysis Process


© 2014- 17, IRJCS- All Rights Reserved

ISSN: 2393-9842
www.irjcs.com

Discrete Cosine Transform (DCT) is used to convert a signal into its basic frequency component. DCT was first introduced by Ahmed, Natarajan and Rao in 1974 in his paper entitled "On image processing and a discrete cosine transform" (Watson, 1994).
DCT has two main properties for image and video compression:

a. Concentrate image energy into a small number of coefficients (energy compaction).
b. Minimizes interdependencies among coefficients (decorrelation).
c. Discrete Cosine Transform of a series of n real s (x), x = 0, ..., n-1, is defined as follows (Watson 1994):

$$S(u) = \sqrt{2/n}\, C(u) \sum_{x=0}^{n-1} s(x) \cos\frac{(2x+1)u\pi}{2n},$$

dengan $u = 0,\ldots,n-1$

dimana $C(u) = \begin{cases} 2^{-1/2}, & untuk\ u = 0 \\ 1, & untuk\ lainnya \end{cases}$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 139 | 144 | 149 | 153 | 155 | 155 | 155 | 155 |
| 144 | 151 | 153 | 156 | 159 | 156 | 156 | 156 |
| 150 | 155 | 160 | 163 | 158 | 156 | 156 | 156 |
| 159 | 161 | 162 | 160 | 160 | 159 | 159 | 159 |
| 159 | 160 | 161 | 162 | 162 | 155 | 155 | 155 |
| 161 | 161 | 161 | 161 | 160 | 157 | 157 | 157 |
| 162 | 162 | 161 | 163 | 162 | 157 | 157 | 157 |
| 162 | 162 | 161 | 161 | 163 | 158 | 158 | 158 |

Pixel Values

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1260 | -1 | -12 | -5 | 2 | -2 | -3 | 1 |
| -23 | -17 | -6 | -3 | -3 | 0 | 0 | 1 |
| -11 | -9 | -2 | 2 | 0 | -1 | -1 | 0 |
| -7 | -2 | 0 | 1 | 1 | 0 | 0 | 0 |
| -1 | -1 | 1 | 2 | 0 | -1 | 1 | 1 |
| 2 | 0 | 2 | 0 | -1 | 1 | 1 | -1 |
| -1 | 0 | 0 | -1 | 0 | 2 | 1 | -1 |
| -3 | 2 | -4 | -2 | 2 | 1 | -1 | 0 |

DCT *Values*

Fig. 5 Pixel Values vs. DCT coefficients

Digital watermarking is a technology to provide and prove ownership rights to digital work, detect legitimate copy, control legitimate data usage and analyze data deployment through network and server. The main purpose of digital watermarking in this paper is to design an algorithm that can be used for all types of video and can embed embedding information type code, especially binary code, in these words. On watermarking, label or code inserted into multimedia data it must be unique to identify the copyright holder and the label is difficult to remove even after multiple data transformations. So the existence of data (label) in the product must be maintained.

Fig. 6 Notice a visible watermark in the form of light gray lettering in the backgroundof the image


© 2014- 17, IRJCS- All Rights Reserved

## III. METHOD

Research on this steganography using LSB (Least Significant Bit) method, analyze LSB in data insertion (message) and analyze image quality from message insertion result. The need used in this research is to insert a message on the image with extension JPEG or BMP. Problems in this research are:

a. Determine Stego System Encoder and Stego System Decoder
b. Analyze message insertion into image
c. Use of stego - key

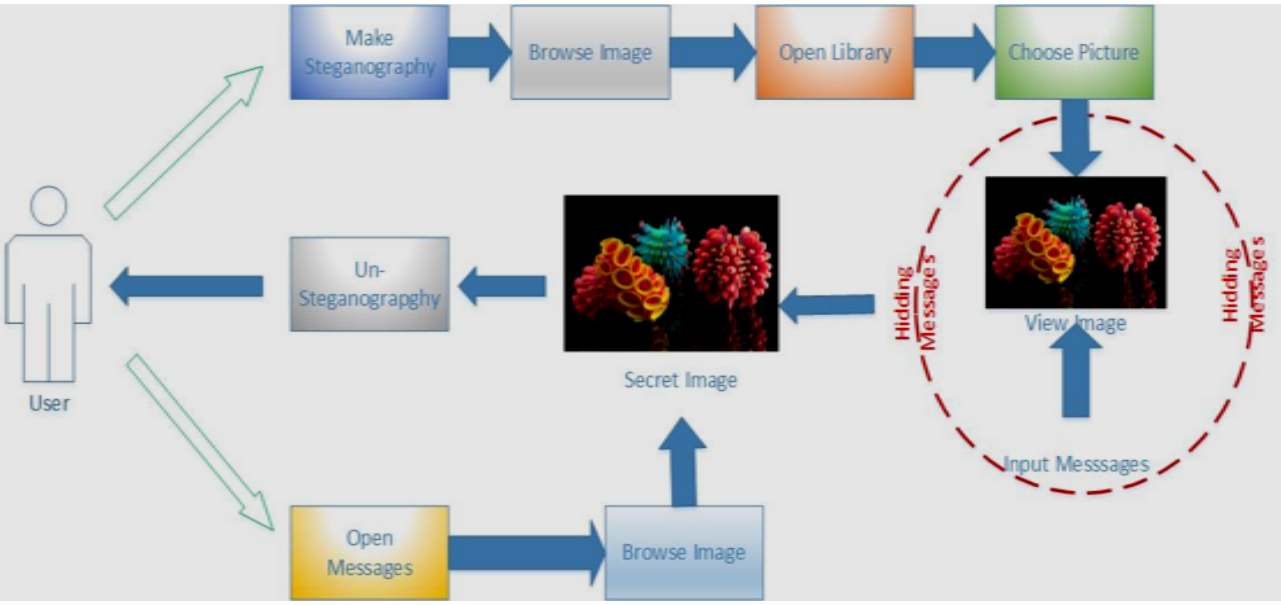


Fig. 7 Conceptual of Steganography

In the picture above explains, that the user (user) in the application has 2 concepts, the first is to create steganography and read the message content from steganography itself. In creating steganography, the user of the first stage is to insert the picture that the message wants to insert.

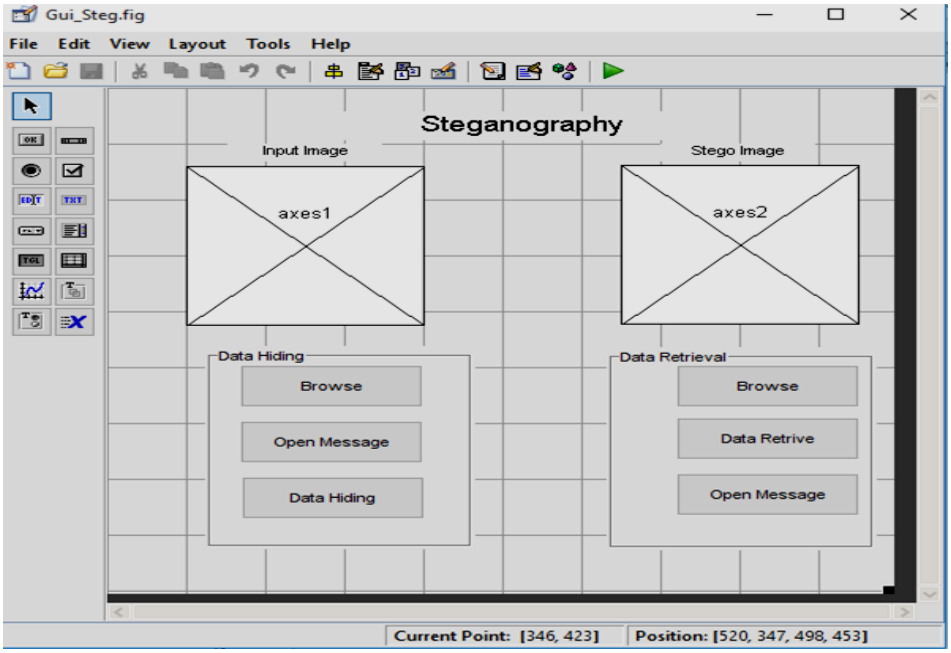


Fig 8. Design of Steganography (Encode Steganography dan Decoder Steganography)

After getting the picture, then user enter the message into the image. Images that have been inserted messages will not change the shape or image memory itself.


© 2014- 17, IRJCS- All Rights Reserved

After the image is inserted, the other person will not know that the picture has been inserted message, until others can open the contents of the message by using steganography application.Implementation to be done is to insert a message on the picture, and the process of inserting the message such as:

a. Message insertion process, in the message insertion process, images that have been inserted messages will not change the shape or memory of the image.
b. The process of taking messages, in the message retrieval process, messages can be retrieved or readable after the user uses a steganography application

## IV. RESULT AND DISCUSSION

From the results of this research has been done, the results obtained from these studies, while the results of research studiess:

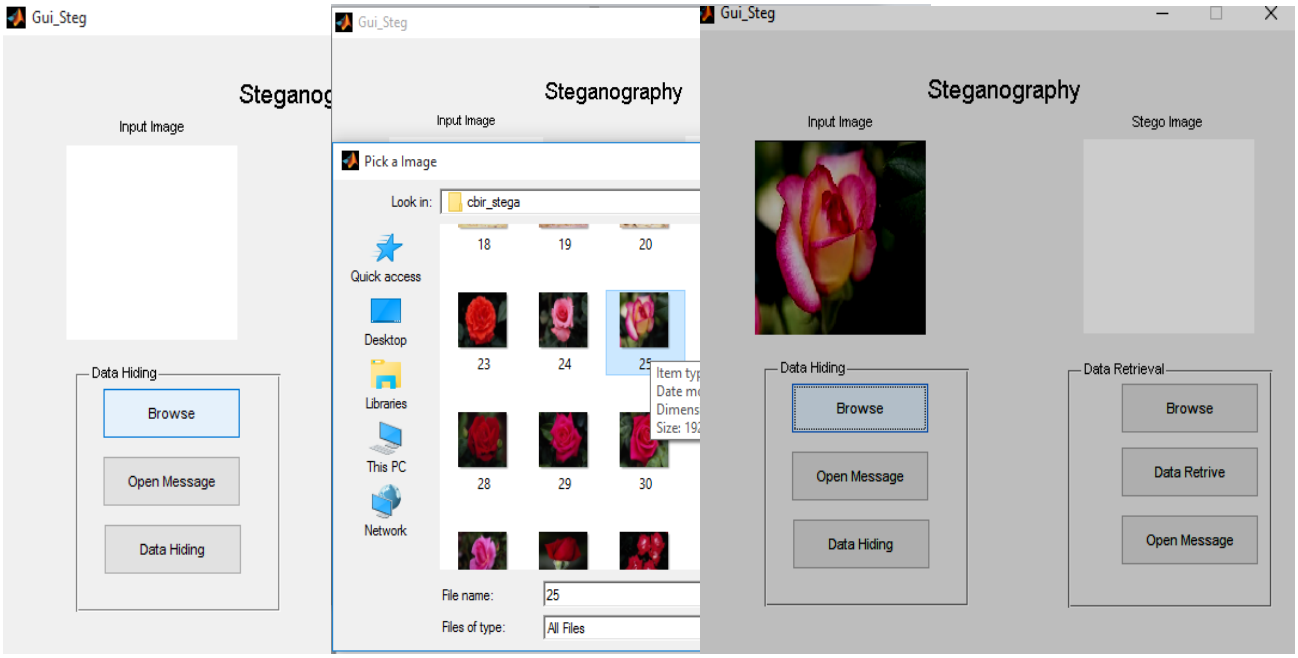


Fig 9. Selecting Images and Displaying Image Selection Results

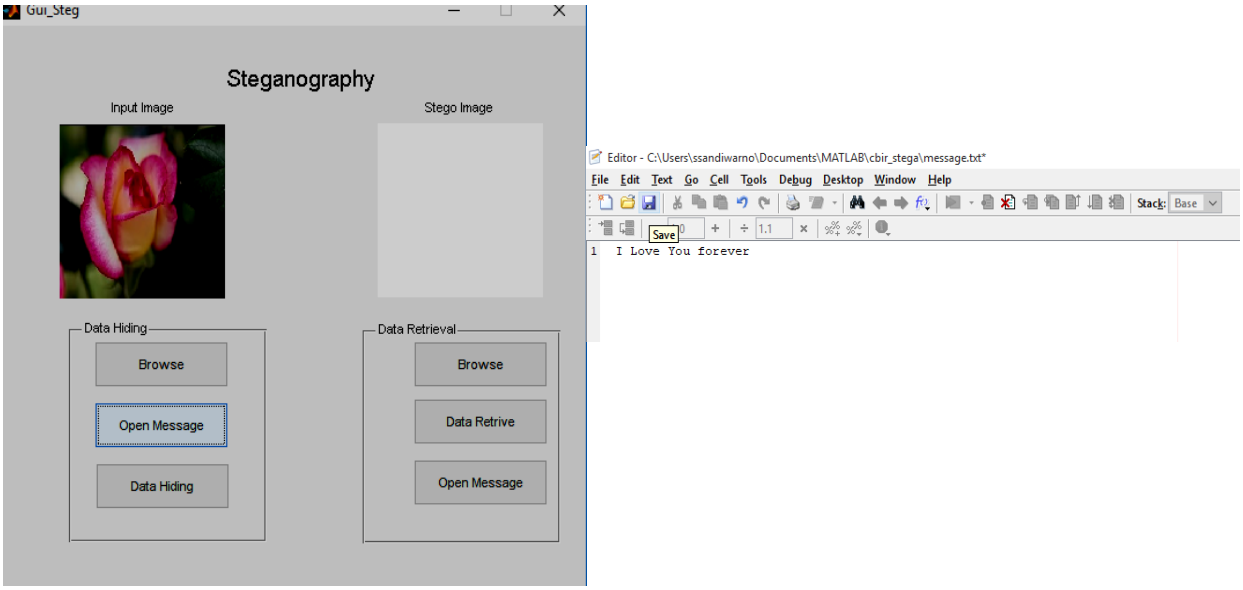


Fig 10. Insert a message inside the picture


© 2014- 17, IRJCS- All Rights Reserved

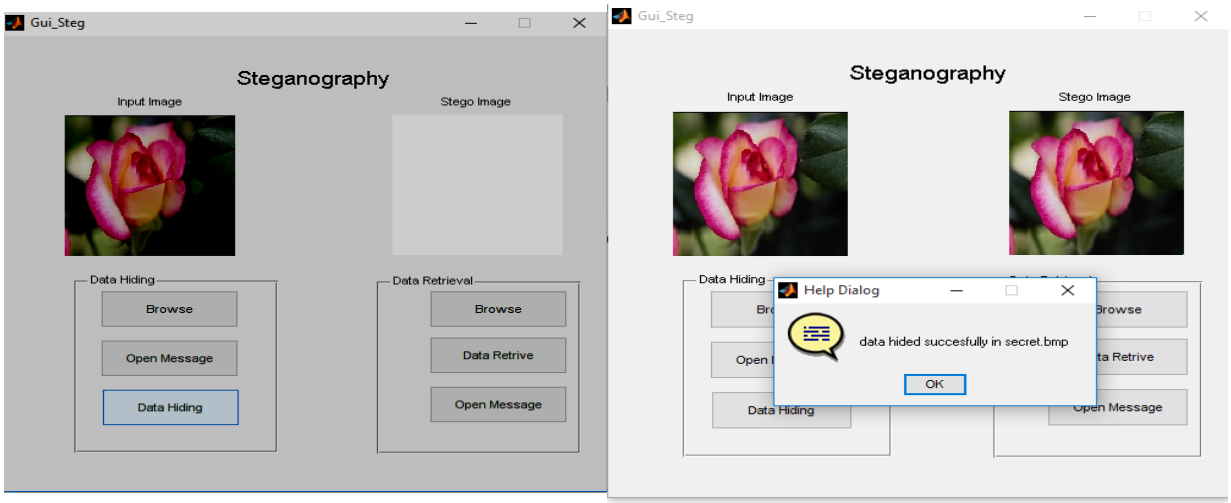


Fig 11. Result of hiding message

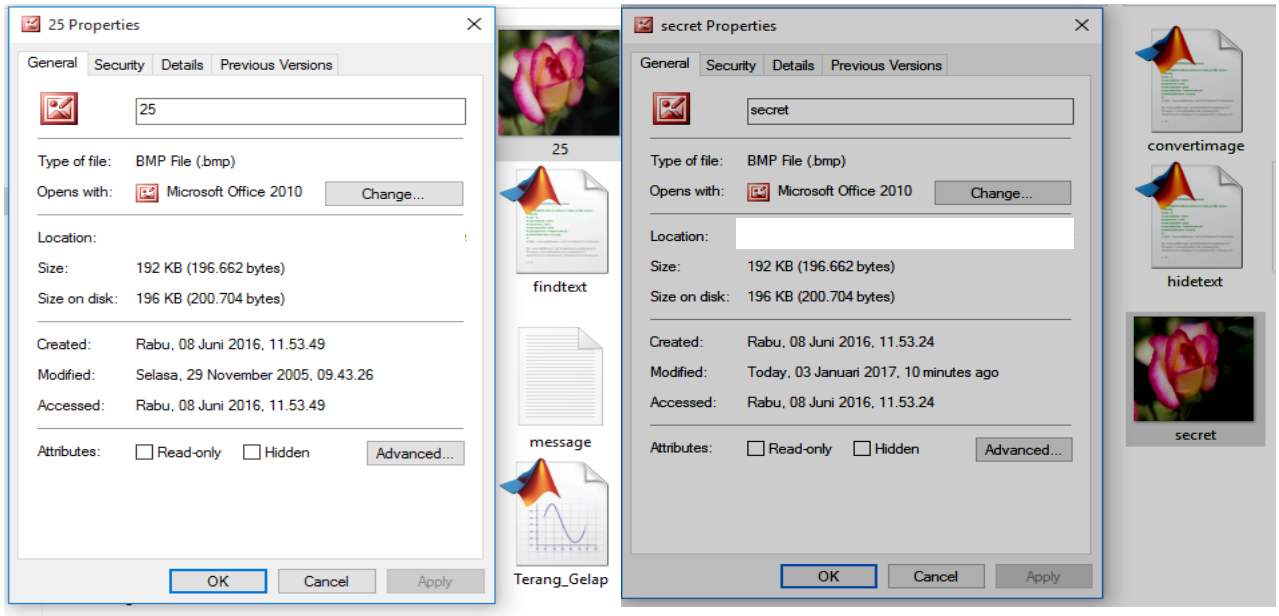


Fig 12. Memory size of the pictures

Description in Fig. 12, explains that 25.bmp and secret.bmp have the same capacity of 192 KB (196,622 bytes). From Fig. 12 it is seen that steganography will not change the shape and image memory and everything remains the same, only if we know that the picture has been inserted message.

## V. CONCLUSION

After doing research on steganography, then got the conclusion, as for conclusion of this research such as:

a. Steganography is an art technique used in the insertion of messages in the media (images, video or music).
b. Steganography has 2 concepts, first is the stego system encoder and stego system encoder. Which means steganography can be used to insert messages, and can also be read the contents of messages from objects inserted messages.
c. The insertion on steganography will not change the shape (texture, color) nor the capacity or memory of the object (images, video or music) inserted messages.


© 2014- 17, IRJCS- All Rights Reserved

ISSN: 2393-9842
www.irjcs.com

## REFERENCES

1. Edward Jero Sam Jeeva Raj AndPalaniappan RAMU, ECG Steganography Using Contourlet Transform For Transmission Of Secured Patient Identity,Proceedings Of The Singapore Cyber-Security Conference (SG-CRC), 2016
2. Eric Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, Inc, Indianapolis, 2003
3. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, Digital Watermarking and Steganography Second Edition, Morgan Kaufmann Publishers, USA, 2008
4. Jeng-Shyang Pan, Hsiang-Cheh Huang, Lakhmi C. Jain and Yao Zhao,Recent Advances in Information Hiding and Applications, Springer-Verlag Berlin Heidelberg, 2013
5. Nedeljko Cvejic, Algorithms For Audio Watermarking And Steganography,University of Oulu, Finland, 2004
6. Peter Wayner, Disappearing cryptography: Information hiding: Steganography & watermarking, Morgan Kaufmann Publishers, USA, 2009
7. Philip Bateman, Image Steganography and Steganalysis, University of Surrey, United Kingdom, 2008
8. Tri Prasetyo Utomo, Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online, Fakultas Sains Dan Teknologi, UIN Sunan Gunung Djati Bandung.


© 2014- 17, IRJCS- All Rights Reserved