IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
ISSN : 2348 - 6090
www.IJCAT.org

Concealing Information using Image Steganography

[1]Akanksha Pawar, [2] Kunali Kharbikar , [3] Gaurav Chaudhari, [4] Amruta Belkhede

[1, 2, 3, 4] Department of Computer Technology, Rajiv Gandhi College Of Engineering & Research,
Nagpur, India

Abstract - Due to exponential growth and secret communication of potential computers users over the internet, the chances of information being detected during the transmission is being an issue now a days. Some solutions to be discussed is how to pass information in manner that the very existence of the message is unknown in order to repel attention of the potential attacker. Beside hiding data for secret communication an approach of information hiding can be extended to copyright protection for digital media. In this paper, we propose modified LSB technique for Image Steganography to hide secret message i.e. Text, Image, Audio and Video in an Image which makes it harder for unauthorised people to extract the original message.

***Keywords* - Cover media, LSB algorithm.**

1. Introduction

Communication of secret information is a critical factor in information technology that continues to create challenges with increasing level of sophistication. When communication takes place between parties that are located on the same secure network, these challenges can be considered as manageable. However ,In the modern era expectations are that one can travel the world and receive secret information at the same time without jeopardizing the confidentiality of secret information. In these situation where the involved parties are spatially separate, the security of secret information cannot rely on the advance technologies of secure network ,and additional security mechanism should be incorporated.

New Steganogarphical technologies have been created to provide security with or without data encryption including data hiding. Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, image, audio and video without causing statistically significant modification to the cover image.

2. Different Types of Steganography

Steganography can be classified into various types depending upon the cover medium used. Hence, Steganography can be said to occur four major types:

1.

1. Text
2. Images
3. Audio
4. Video

2.1 Text Steganography

Hiding information in text is historically the most important method of steganography. A simple method was to hide the secret message in every nth letter of every word of a text message. Due to the beginning of the internet and due to different types of digital file formats it has decreased in importance. Text steganography using digital file is not used very often because the text files have a very small amount of redundant data.[1]

2.2 Image Steganography

Images are the most popular cover objects for steganography[1].A message is embedded in a digital image(cover image) through an embedding algorithm by using secret key. The resulting stego image is transmitted to the receiver. On the other hand ,it is processed by the extraction algorithm using the same key. During the transmission of the stego image, it can be monitored by some unauthenticated person who will only notice the transmission of an image but cannot guess the existence of the hidden image

2.3 Audio steganography

Audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound becomes inaudible in the presence of another louder audible sound. This property allows to select the channel in which to hide information. Although it is similar to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images.[1]

2.4 Video Steganography

Video steganography is a technique to hide any kind of files or information into digital video format. Video (combinations of picture) is used as a carries for hidden information. Generally discrete cosine transform (DCT) alter values (e.g. 8.667 to 9) which is used to hide information in each of the images in the video, which is not noticeable by human eye. Video steganography uses such as H.264,MP4,MPEG,AVI or other video formats.[2]

Many Experiments have been made on different types of host files and also the secret message and following combinations are most successful:

Table-1 Cover file type and secret message file type [3]

S. No.	Cover file type	Secret file type used
1.	.BMP	.BMP,.DOC,.TXT,.WAV,.MP3,.XLS,.PPT,.AVI,.JPG,.EXE,.COM
2.	.JPG	.BMP,.DOC,.TXT,.WAV,.MP3,.XLS,.PPT,.JPG,.COM
3.	.DOC	.TXT
4.	.WAV	.BMP,.JPG,.TXT,.DOC
5.	.AVI	.TXT,.JPG,.WAV
6.	.PDF	.TXT

From this table, we can prefer images as the best cover media for hiding messages.

3. Basic Model

In the following diagram, the basic approach is given:

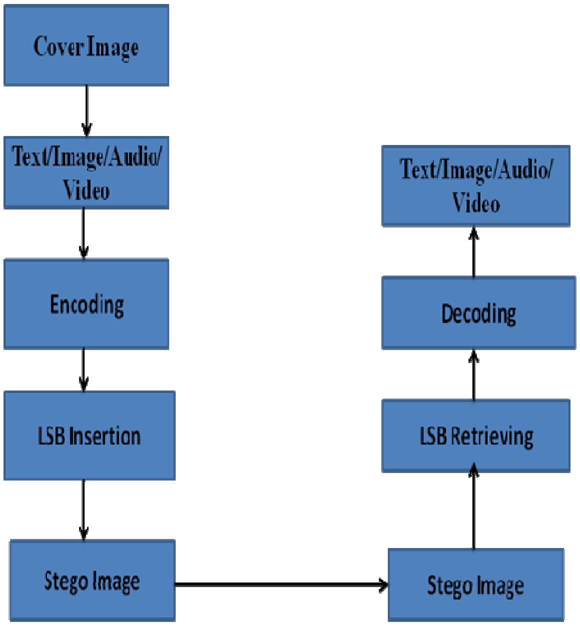


Fig1:Flow of the model (insertion and retrieving process)

4. Methodology

4.1 Least Significant Bit (LSB) Technique

LSB insertion is a common and simple approach to embed information in an image file. In this method the LSB of a bit is replaced with an M's bit. This techniques works good for image steganography .To the human eye the stego image will look identical to the carrier image. For hiding information inside the images, the LSB method is usually used. To a computer an image file is simply a file that shows different colours and intensities of light on different areas of an image. [4].

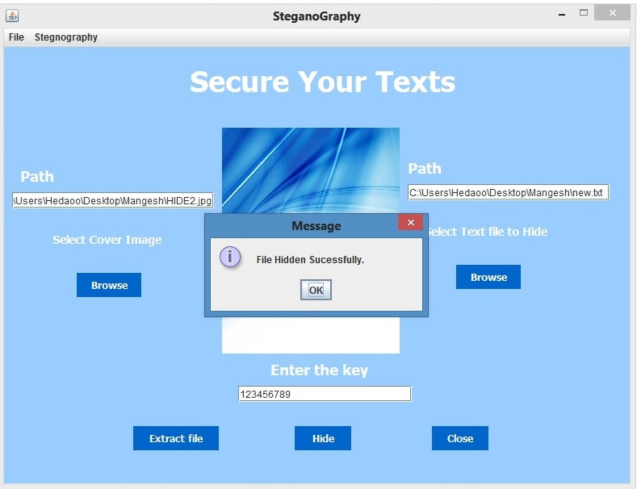
For example, We are embedding alphabet A inside some raster data-
A sample raster data for 3 pixels (9 bytes) may be:
00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101011

2. ↓ Inserting the binary value of
3. A
4. (1000001)
5. 0010011**1** 1110100**0** 1100100**0**
6. 0010011**0** 1100100**0** 1110100**0**
7. 1100100**0** 0010011**1** 11101011

4.2 Modified Least Significant Bit

Text and Images can be hidden behind the cover image by using LSB technique. While hiding audio and video files behind cover image, we have chosen to replace not just LSB but also LSB+1 bit so that these file which have comparably large size as compared to text/image file can be hidden successfully. Here we are implementing LSB technique in a modified way so as to accomplish our task and hide the files behind the cover image without any data loss.

5. Screen Shots



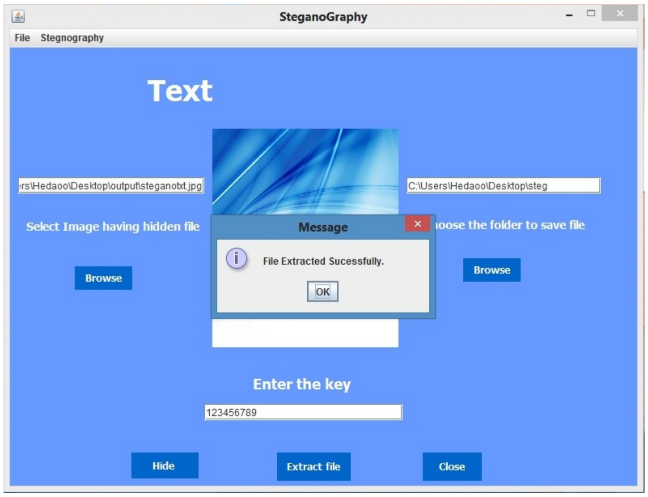
\Users\Hedaoo\Desktop\Mangesh\HIDE2.jpg

C:\Users\Hedaoo\Desktop\Mangesh\new.txt

File Hidden Sucessfully.

123456789

Fig2: In this figure,cover image is chosen and file i.e. text which is to be hidden is selected and hidden successfully.



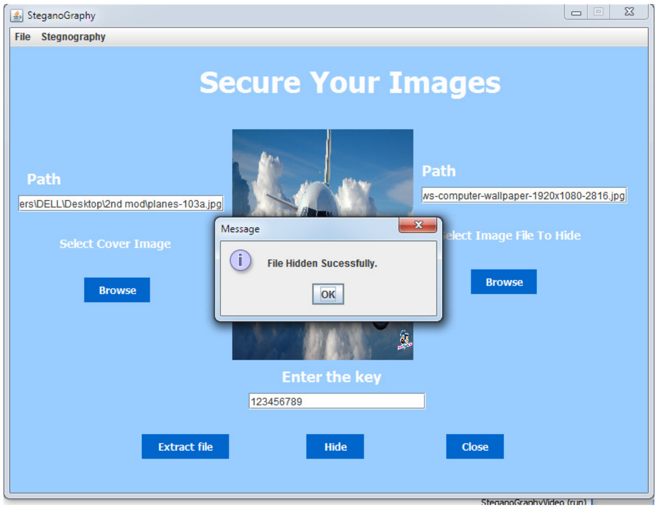
rs\Hedaoo\Desktop\output\steganotxt.jpg

C:\Users\Hedaoo\Desktop\steg

File Extracted Sucessfully.

123456789

Fig3:In this figure,stego-image is selected and the folder location is selected where the hidden data i.e text will be saved.



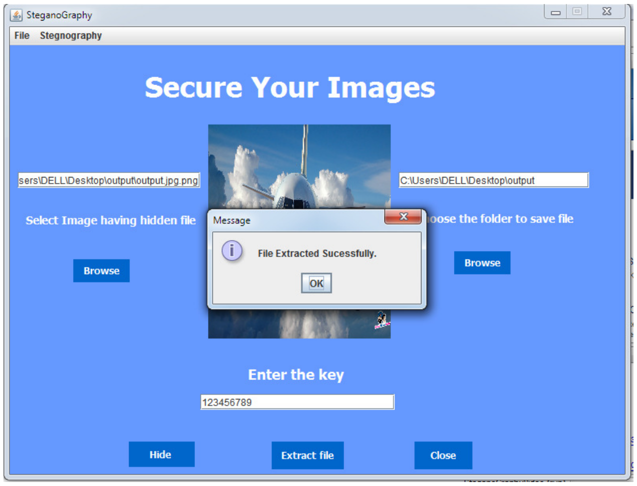
ers\DELL\Desktop\2nd mod\planes-103a.jpg

ws-computer-wallpaper-1920x1080-2816.jpg

File Hidden Sucessfully.

123456789

Fig4: In this figure,cover image is chosen and the file i.e. image which is to be hidden is selected and hidden successfully.



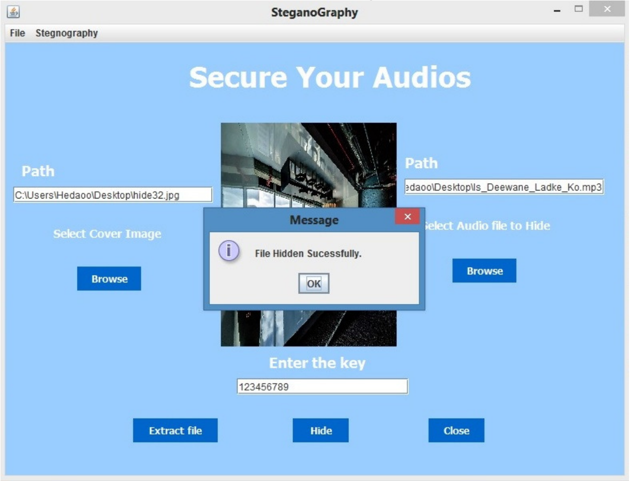
sers\DELL\Desktop\output\output.jpg.png

C:\Users\DELL\Desktop\output

File Extracted Sucessfully.

123456789

Fig5:In this figure,stego-image is selected and the folder location is selected where the hidden data i.e image will be saved.



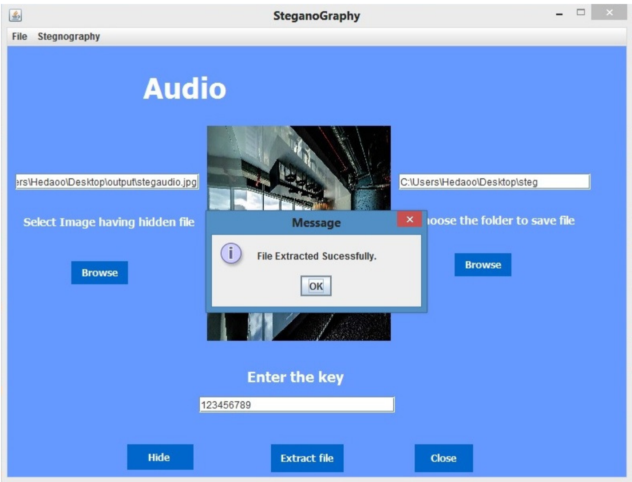
C:\Users\Hedaoo\Desktop\hide32.jpg

edaoo\Desktop\Is_Deewane_Ladke_Ko.mp3

File Hidden Sucessfully.

123456789

Fig6: In this figure,cover image is chosen and file I.e audio which is to be hidden is selected and hidden successfully.



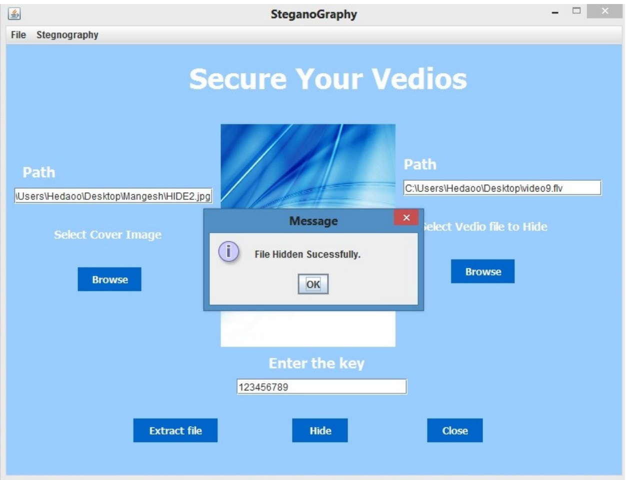
rs\Hedaoo\Desktop\output\stegaudio.jpg

C:\Users\Hedaoo\Desktop\steg

File Extracted Sucessfully.

123456789

Fig7:In this figure,stego-image is selected and the folder location is selected where the hidden data i.e audio will be saved.



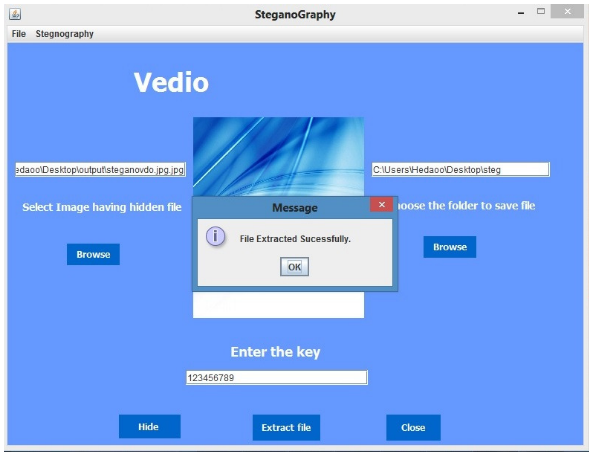
\Users\Hedaoo\Desktop\Mangesh\HIDE2.jpg

C:\Users\Hedaoo\Desktop\video9.flv

File Hidden Sucessfully.

123456789

Fig8: In this figure,cover image is chosen and file i.e. video which is to be hidden is selected and hidden successfully.



edaoo\Desktop\output\steganovdo.jpg.jpg

C:\Users\Hedaoo\Desktop\steg

File Extracted Sucessfully.

123456789

Fig9:In this figure,stego-image is selected and the folder location is selected where the hidden data i.e video will be saved.

6. Applications of Steganography

A. Spies: Intelligence and counter intelligence agencies.
B. Militaries: Unobtrusive communication.
C. Terrorist: It arouses less suspicion.
D. Copyright: Watermarks and fingerprints.
E. Spam: Email forgery.

7. Conclusion

In this paper we gave an overview of steganography. It can enhance confidentiality of information and provides a means of communicating privately. We have also presented image steganographic system wherein we have hidden information behind image using LSB approach. The information can be any image, text, audio, video file. LSB technique replaces the least significant bit with the message to be encoded. It directly embeds the secret data within the pixel of cover image.

The advantage of LSB is its simplicity to embed the bits of the message directly into LSB plane of cover image. Another advantage is its perceptual transparency whereby the changes made to the cover image cannot be traced by human eye. We have chosen LSB because of its ubiquity among carrier formats and message types.

References

[1] Ramanpreet Kaur, Prof. Baljit Singh, “Survey and Analysis of various Steganographic Techniques” , ISSN:2250-3676, Volume-2, Isuue-3, 561-566.

[2] T. Morkel, J.H.P. Eloff, M.S. Olivier, “An Overview Of Image Stegnography”, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[3] Mehdi Hussain and Mureed Hussain, “A Survey of Image Steganography Techniques” , International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[4] Joyshree Nath, Asoke Nath, “Advanced Steganography Algorithm using Encrypted secret message”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[5] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, “Enhanced Least Significant Bit algorithm For Image Steganography”, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN (Online): 2230-7893, www.IJCEM.org.