IJCSE International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-3 E-ISSN: 2347-2693

Hiding Existence of Communication Using Image Steganography

Swati Nimje[1*], Amruta Belkhede[2], Gaurav Chaudhari[3], Akanksha Pawar[4] and Kunali Kharbikar[5]

[1*,2,3,4,5] *Student, Department Of Computer Technology*

Rajiv Gandhi College of Engineering & Research, Nagpur, India

www.ijcseonline.org

Received: 6 March 2014 Revised: 17 March 2014 Accepted: 22 March 2014 Published: 30 March 2014

Abstract— Now a day, maintaining the security of the secret information has been a great challenge. Sending message habitually through a communication channel like internet draws the attention of third parties and hackers, perhaps causing attempts to break and expose the sent messages. 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. Besides 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— Stego-File, Cover-Image, Modified LSB

I. INTRODUCTION

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorised access. This has resulted in an explosive growth of the field of information hiding.

Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately, it is sometimes not enough to keep the contents of message secret, it may also be necessary to keep the existence of message secret. The technique used to implement this is called Steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communication information. Image Steganography 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.

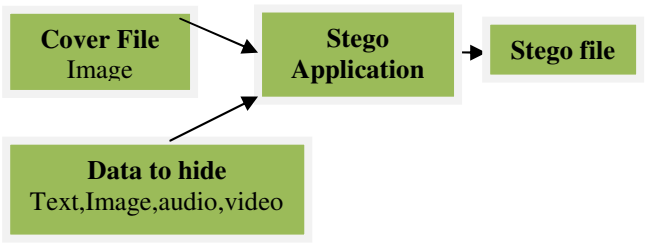


Figure: Steganography Process

Corresponding Author: *Swati Nimje*

II. TYPES OF STEGANOGRAPHY

Steganography can be classified into various types, depending upon the cover of medium used. Hence, steganography can be set to occur in five types:

1. Text
2. Image
3. Audio
4. Video
5. Protocol

II-A. 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 n^{th} 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]

II-B. 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

II-C. 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 steganography potential, the larger size of meaningful audio files makes them less popular to use than images.[1]

II-D. 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]

II-E. PROTOCOL STEGANOGRAPHY

The term protocol steganography refers to embedding information within network protocols such as TCP/IP. An example of it is hiding information in the header of TCP/IP packet in some fields that can be either optional or are never used.

Many Experiments have been made on different types of cover files and also be secret message and following combination are most successful:

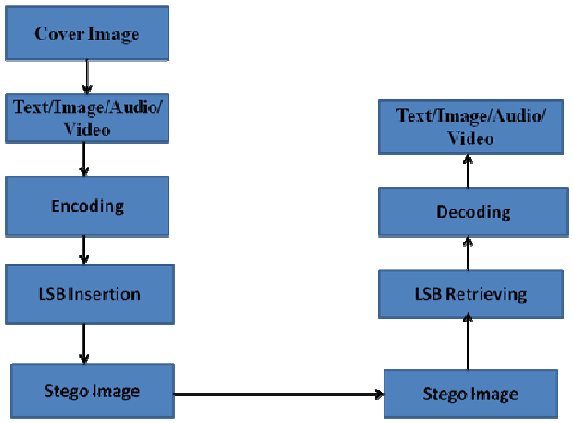
Table -1 Cover file type and secret message file type [3]

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.

III. BASIC MODEL

The basic approach is given in the following diagram



IV. METHODOLOGY

IV-A. LEAST SIGNIFICANT BIT TECHNIQUE: LSB insertion is a common and simple approach to embed information in an image file. In this method LSB of a bit is replaced with an M's bit. This technique works good for image steganography t 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 show a different colours of intensities of light on different areas of an image [4.5].

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

Inserting the binary value of A

(1000001)

00100111 11101000 11001000

00100110 11001000 11101000

11001000 00100111 11101011

IV-B. MODIFIED LEAST SIGNIFICANT BIT:

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

V. RESULTS

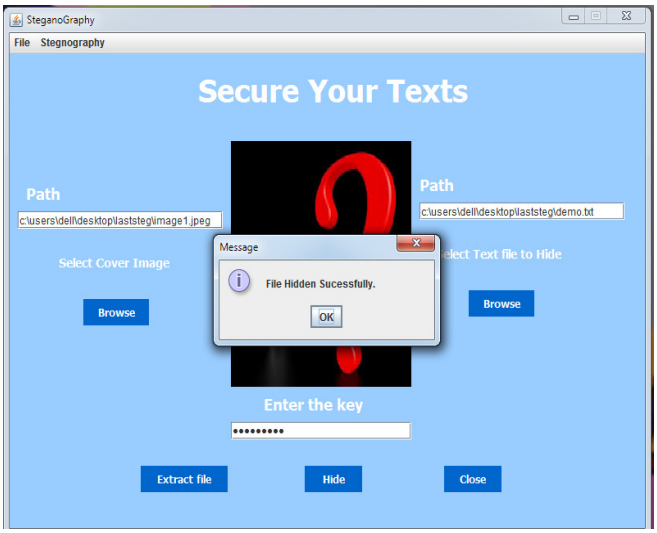


Fig: Text file hidden behind cover image

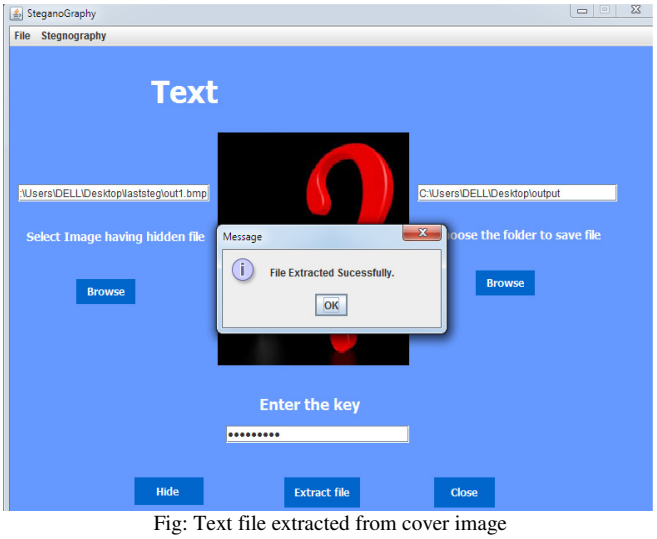


Fig: Text file extracted from cover image

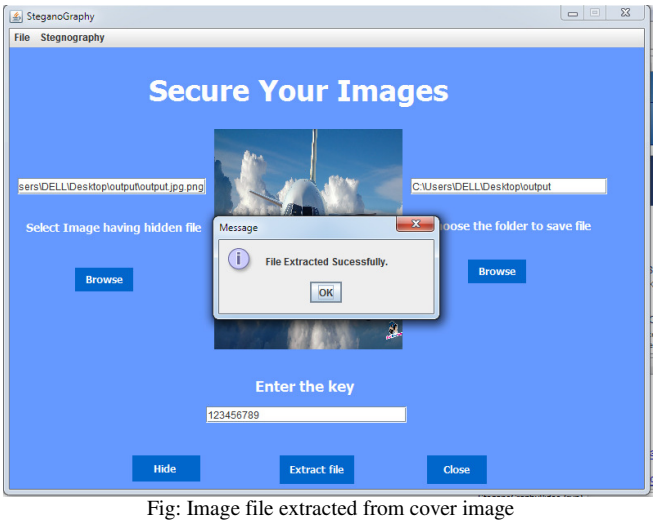


Fig: Image file extracted from cover image

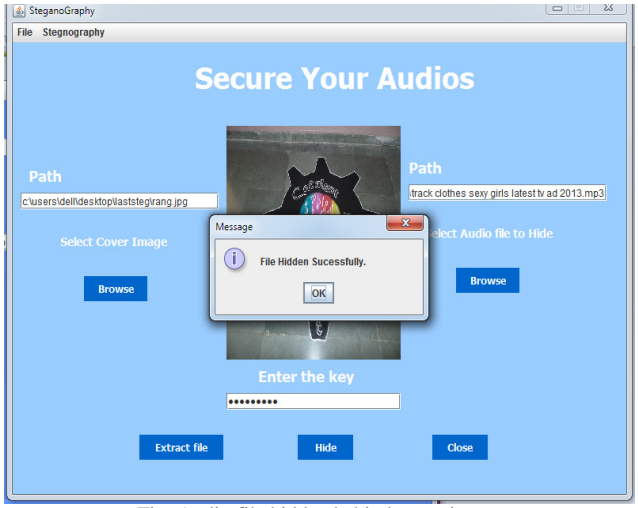


Fig: Audio file hidden behind cover image

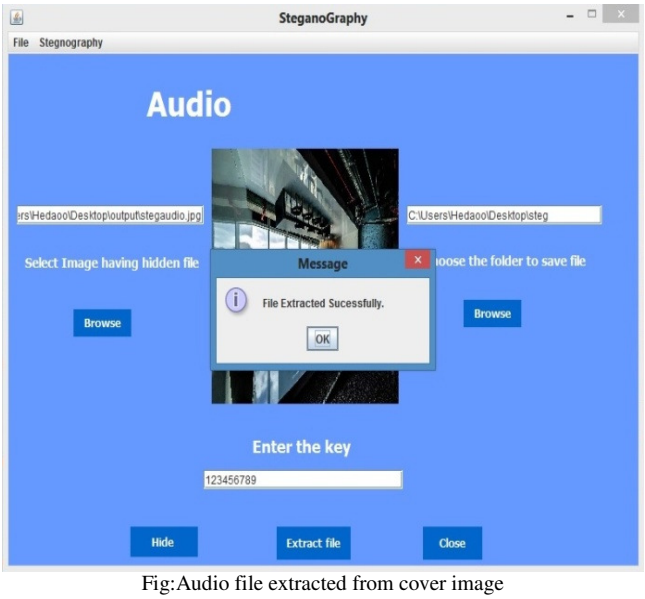


Fig:Audio file extracted from cover image

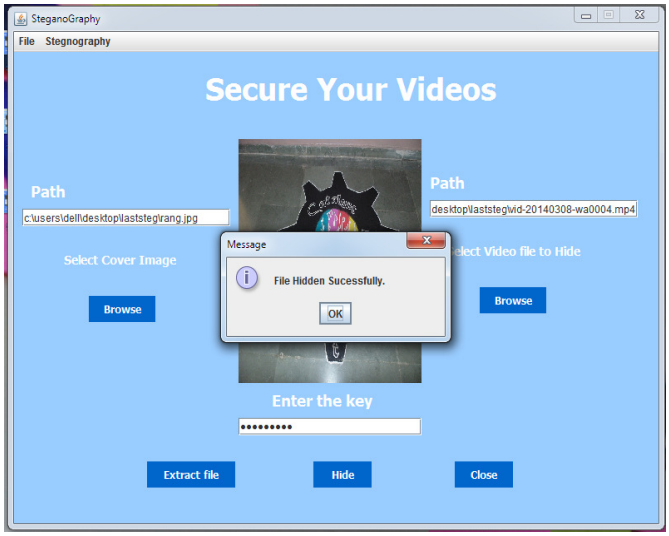
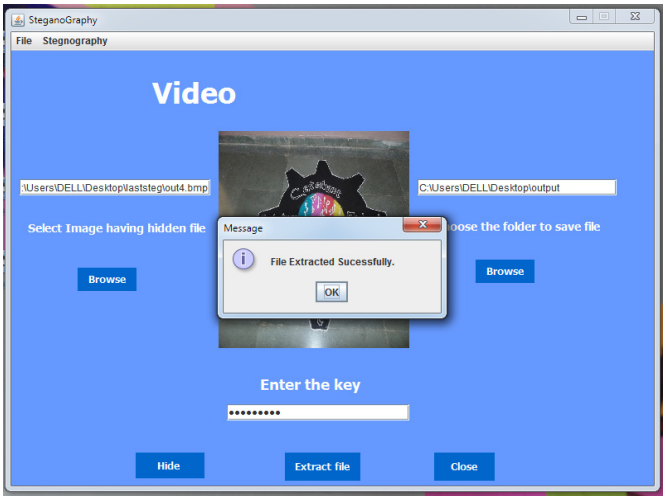


Fig: Video file hiding behind cover image



VI. APPLICATION

1. Spies: Intelligence and counter intelligence agencies.
2. Militaries: Unobstructive communication.
3. Terrorist: It arouses less suspicion.
4. Copyright: Watermarks and fingerprints.
5. Spam: Email forgery.

VII: CONCLUSION

It can enhance Confidentiality of information and provides a means of communicating privately. We have also presented image steganography system wherein we have we have hidden information behind image using LSB approach. The information can be any image, text ,video ,audio file.

LSB technique replaces the significant bit with the message to be encoded; it directly embeds the secret data within the pixel of cover image.

The advantage f 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

AUTHORS PROFILE

Name:Swati Nimje

Name:Amruta Belkhede

Name: Gaurav Chaudhari

Name:Akanksha Pawar

Name:Kunali Kahrbikar