An Insight Into The Working And Application Of Steganography

Sourjya Sen [#1], Mukul Varshney [*2]

Amity Institute of Telecom Engineering and Management, Amity University, Noida Sector-125,India
[1] sourjya.sen@student.amity.edu
[2] mvarshney@amity.edu

Abstract— **Steganography is an artistry of hiding information. It is the process where one message is hidden in another message. Where as in cryptography we format the message in such a manner that it cannot be consumed by an intruder or a person for whom the message is not meant for .Where as in case of steganography it will show a fake, useless but consumable message to the person for whom the message is not intended this will cause the lack of suspicion due to which the number of attempts to attack the secret message will be less. Hence the no. of attempts to decrypt the message will drastically reduce, by unwanted party. The main advantage of this procedure is the lack of suspicion. This consequentially increase the security of the text file that we want to send to specific individuals and hence conclusively we can say that, steganography is more safe and reliable as compared to other traditional ways of encryption and decryption**

Keywords : Steganography, Least Significant Bit Technique (LSB)

I.   INTRODUCTION

There are various types of information in general whether it is in the digital world or the physical word. We can consume information in variety of ways by seeing and listening like through radio, television newspapers and various other forms of consumable media as we observe But for example If one person, let's say person A wants to communicate with person B and that person wants it between the two parties in general and wants it to be coveted and secret one way is to go and secretly tell person B but If A also wants to remove suspicion as far as possible then he might give person B that message in such a way that even if other people are suspicious at first they observe and see some random useless information sharing is happening so suspicion is removed hence no one in general will even try to get the information in general as they will think they know what is the information which is being shared but actually they know only false information not real one. We are basically using the most basic form of digital information that is 0 and 1 also known as bits and we are converting both image and textual information into that for encrypting them together to form a new image basically a kind of smoke screen information in general to fool people those for whom information is not intended and then just put out for whom it is required and they get the real information by necessary ways applied to get the required information for the message consumption.

II.   METHOD USED

We have explored and exploited one of the basic techniques of encryption i.e. LSB (Least Significant Bit) We have used txt files and bmp files combination to generate a bmp file by first converting the txt files and bmp files in 0 and 1 binary bit format and encrypted them together to form the new bmp file in general which will have the hidden message in general we use a certain methodology and logic application for encryption and decryption process and to fulfill the task to get the image in general

The important ,secret message the type of message which is intended for few specific kinds of people in general is first is going to be converted into bits by using reading functions of java program for reading files in general this kind of thing is going to happen to both respective types of text and image it will be used for bmp image type of file because it works with bmp image file only in general for the basic simple functioning of the system that is going to be used for this specific type or kind of information exchange between 2 different kind of individuals or groups sects etc. So, basically saying that this system in the beginning is going to change the message file or text file in .txt format is going to be converted into bits that are the format of 0 & 1 and then the image which is going to be in the bmp format will also be converted into bits. This will be done by using the respective functions of java programming that is going to help us in achieving our goal by completion of the initial stages of project and then moving on forward and similarly decrypt it from bits .The beauty of this project will be that it will not affect the appearance of image at all .This further help in removal of suspicion of secret important kid of information
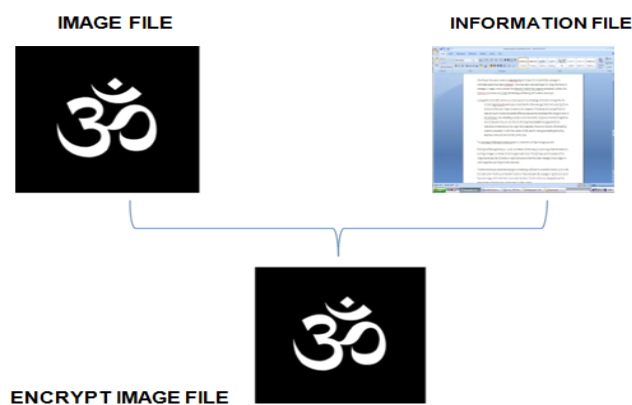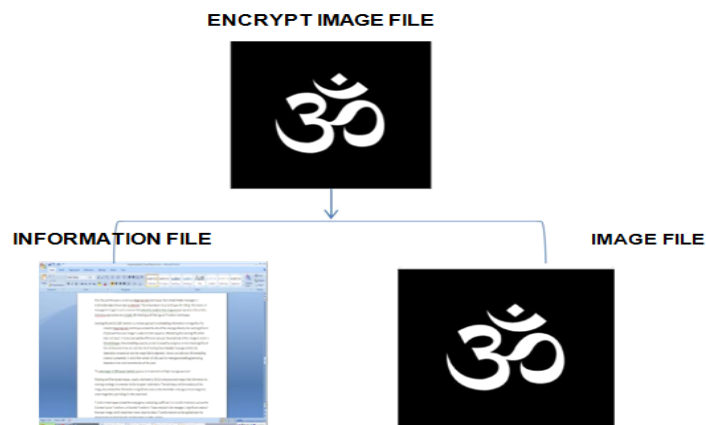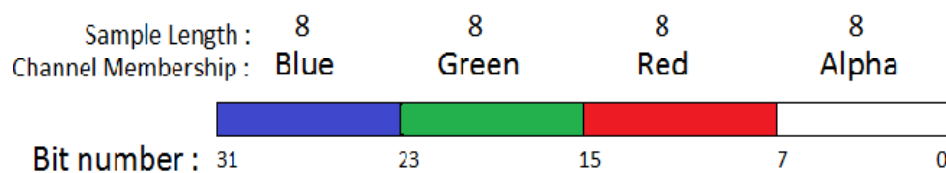

The text file is taken as input and converted into the binary bytes of stream.

Now, each bit of these bytes is encoded in the LSB of each next pixel using ARGB.

Since only Alpha part of ARGB used hence 0.39 % of the pica is going to be impacted upon

We have used Java Programming using features like Swings buttons files Input stream output stream etc to do our work

III.   RESULT

The Respective figures are basically representing the three cornerstones of the project that's has been made

Figure 3 shows the main menu that will appear after running the java code It shows three options respectively that is cipher file decipher file and exit menu .The user will click the intended option in the menu within such as cipher file option is clicked upon a panel form type appears asks for the detail the browse button is clicked a menu appears from where the respective file is chosen

First one is going to be for the text file second one for the image file and third one asks name and location desired by user for the file/image that is going to be generated after the encryption of image and text bits respectively and the new image is generated

Similarly we click decipher file we get decryption menu asks for the encrypted image and desired location for decrypted text that is required

The user clicks ok and gets the required message which is of value to the user this is that secret kind of message which is only intended for the certain kind of users or people in general

Finally the respective file icons generated with respect to the panels and the locations in which they are going to be placed as specified by the program and the details that are filled by the user in the respective panels
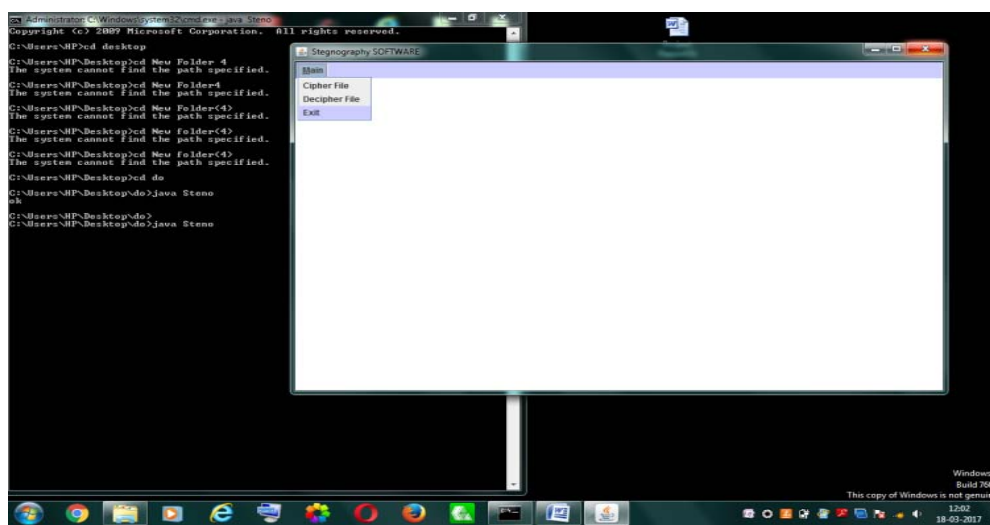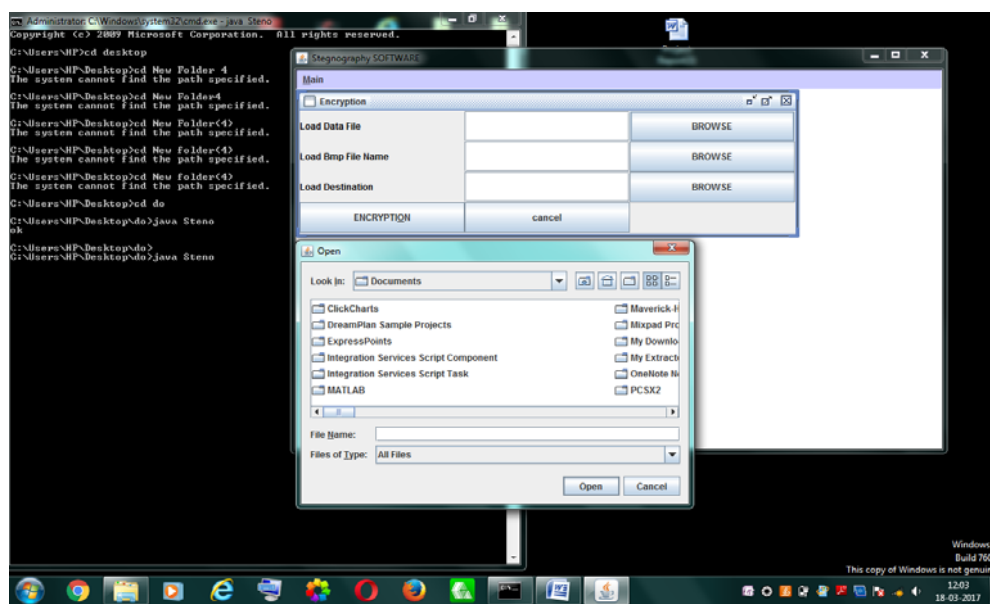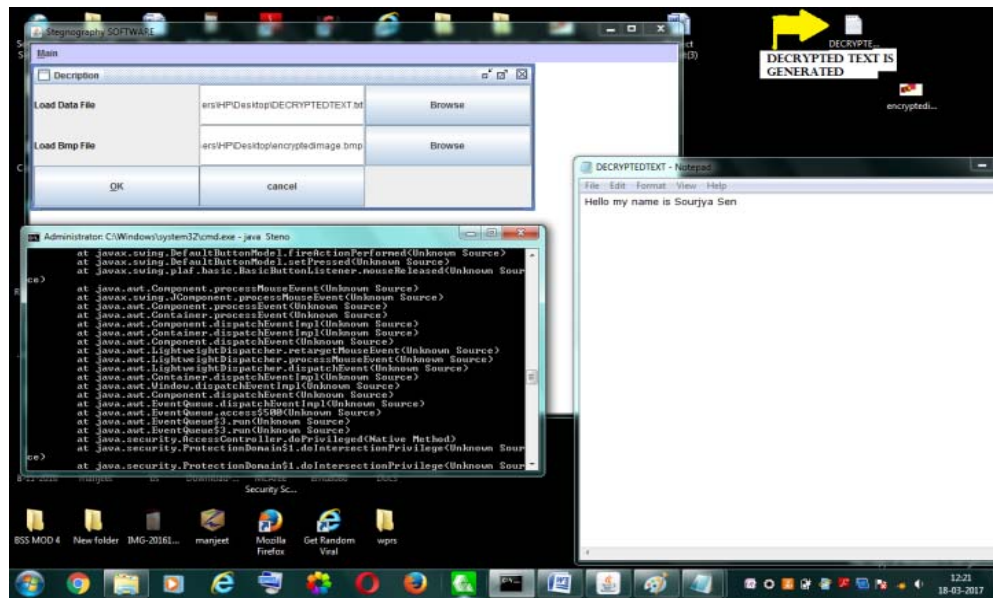

Figure :Menu

Figure :Encryption Panel

Figure : Decryption Pane

IV. CONCLUSION

This paper shows a miniscule view on the field of steganography. This will show how steganography work's at a ground level. It can be assumed that steganographical communication is not a traditional way of coveted communication via the internet. It 's biggest asset is that it has lack of suspicion due to which less attacks hence security increases by many field as shown in this paper

ACKNOWLEDGMENT

REFERENCE:

[1] Donovan Arts, Los Alamos National Laboratory, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing: May, 2001.
[2] Chinchilla A.A. And Rude D.A., Design And Implementation Of Image Steganography, Journal of Signal and Image Processing, Volume 3, Issue 3, 2012, pp.-111-113.
[3] Programmers Heaven, http://www.programmersheaven.com/mb /java/369382/369382/creating-a-bmp-in-java, Accessed on Feb. 13, 2010.
[4] Pierre Richer, "Steganalysis: Detecting hidden information with computer forensic analysis", SANS Institute InfoSec Reading Room, 2003.
[5] This Could Be Better, http://thiscouldbebetter.wordpress.com/2011/08/16/reading-and-writing-a-bmp-file-using-java, Accessed on Feb. 13, 2010.
[6] T. Morkel, J.H.P. Eloff, M.S. Olivier, An Overview Of Image Steganography, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa, http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/098_Article.pdf
[7] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, "Digital Watermarking and Steganography", Morgan Kaufmann Publishers, Elsevier, 2008.

[8]   Gary C. Kessler, "Steganography: Hiding Data within Data", September 2001, http://www.garykessler.net/library/steganography.html, Accessed on Feb 20, 2010.
[9]   Computer Forensics, Cybercrime and Steganography Resources, http://data-hiding.com, Jan. 14 2010.
[10] Johnson & Johnson Technology Consultants, LLC, http://www.jjtc.com/Steganography, Accessed on Jan. 20, 2010.
[11] developer.com, http://www.developer.com/java/ent/article.php/3530866/ Steganography-101-using-Java.htm, Feb 13, 2010.

AUTHOR PROFILE

Sourjya Sen is a Student of BTECH Electronics and Telecommunications in Amity Institute of Telecom Engineering and Management in Amity University Noida

Mukul Varshney is currently working as an Assistant Professor in Amity Institute of Telecom Engineering and Management in Amity University Noida