Design & Development Of A System For Hiding Information Within Images Using Steganography

Suhail Shaikh[1], Naima Arshad[2], Areez.khalil[3],Ghazala Shafi Sheikh[4], Ghous Baksh Narejo[5]

Indus University, Karachi (Suhail.shaikh@live.com)

Indus University, Karachi (Naima.Arshad@indus.edu.pk)

Indus University, Karachi (Areez.memon@indus.edu.pk)

Indus University, Karachi (ghazala.shafi@indus.edu.pk)

NED UET, Karachi (ghousnarejo@gmail.com)

Abstract: Steganography is a skill of transfer secreted data or secret messages over an open network so that a third party cannot detect the presence of the secret messages. Nowadays Internet is the most widely used source of communication in the world. Threats to information security have been rapidly increasing in the recent times. Our development to hide information within images using steganography is a contribution to internet security which gives benefit to all the users around the world who think that sending confidential data has become a risk for them. The development objectives to serve as a foundation to create a secure path for transmitting confidential data without the fear of it getting hacked. Our development presents an investigation on several information hiding methods in steganography and evolution of several current image steganography methods of information hiding.

.

Keywords: Steganography, internet, data.

I. INTRODUCTION

As the name "hiding information within digital images using steganography" suggests, the main target of this project is making data transmission safe and secure. For which we have developed a windows application for laptops and Personal computers. Image steganography can be considered as a combination of image processing and communication security. Our target is to hide information (text or word file) in an image in such a way that the face of the original image does not change and human eye cannot detect that something is hidden behind it. Several factors which are significant while designing such an application include the format of the image, the file size, the amount of data that can be hidden, change in pixels of the image, robustness etc. A variety of steganography techniques are available each having their strong and weaker points. Different techniques can be used depending on the type of application by the user.

II. OVERVIEW OF INTERNET SECURITY

Computers and networks were developing to provide ease and help for information sharing and transfer. Initially it was for mainframes and central unit. Then the moves to personal computers and now world is dealing with smart phone and other electronics items.

As the technology is becoming advance the crime is developing also. In past times, to avoid attacks password was commonly used but now only password is not enough. In security Section the development is quite fast now different encryption and decryption techniques, security software and protection are now available.

III. SECURITY THREATS

In this we will discuss different type of security threats. There are two basic threats Natural disasters, Human threats.

IV. NATURAL DISASTERS:

No one can change or control nature. Due to natural disasters information technology faces many problems. Due to natural disasters computer networks gets jammed and do not work properly. This causes information loss, and hardware system destruction. This can't be completely avoided but its effect can be reduced to minimum level and by preparing security plans for disasters.

V. HUMAN THREATS

In human threats cracking, hacking and other attacks by humans mean are kind of human threats. These threats are also known as malicious threats. These attackers have so motive behind their attacks. They can be using hacked information for their benefit or to destroy other reputations. There are different human threats that are classified as.

Viruses
Trojan horse
Worms
Password hacking E-
Mail hacking
Impersonation
Eavesdropping
Packet reply
Packet modification
Network spoofing

VI. IMAGE STEGANOGRAPHY

Steganography is a Greek word which itself is a combination of 2 words "stegos" which means covered and "graphy" which means writing or drawing. Hence both combine to form the title "covered writing basically steganography is the art of hiding information

in other information. It hides the fact that communication is taking place. There are two materials that exist in steganography first is the message and second is the carrier. Message is obviously the secret message we want to embed and carrier is the medium which is going to take that message within it. There are cases when a person cannot send messages openly because of the level of confidentiality of the data. In such cases steganography comes into action and makes sending confidential data secure. Due to advancements in the field of technology most of the data is kept electronically, due to which the security of data has become a fundamental issue. As the number of data being exchanged on the internet increases, information security is becoming more important and hence the need of steganography is also growing.

The main advantage of steganography is that it hides information with such little changes in the original file which cannot be noticed by the human eye.

Hence the before and after image of the stegno file is nearly the same. Nowadays different techniques are used to make data secure which include watermarking, fingerprinting, and cryptography etc. steganography has an edge over all these techniques because it not only makes the information imperceptible but also undetectable. Steganography can be done in various formats like videos, images, and audio files etc. different techniques are also available used to hide data in different ways.

VII. TYPES OF STEGANOGRAPHY

Since steganography works by hiding one type of information into another type of information, hence the medium which we want to hide and the medium in which it is going to be hidden can be of different types. The mediums used electronically for the transmission of information include text, images, audio and videos. Among which text is the most famous and most widely method used to convey messages. Hence there are different types of steganography techniques present. The user can use them according to his/her requirement. Detail of different types of steganography is given below:

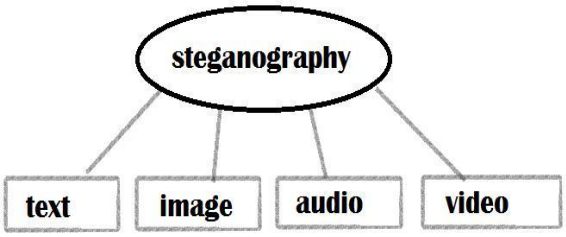

Fig. 1 Types of steganography.

A. IMAGE STEGANOGRAPHY:

Nowadays a new technique is hiding information within a digital image, a message when hidden inside an image can easily be sent via various sources online. The practical use of steganography is still limited because of the lack of awareness among people about its benefits. Just like text steganography image steganography can also be performed by various techniques which we will discuss later, as our project is mainly based on image steganography. To hide a message inside an image without altering the physical properties of the image is the main challenge while performing steganography on images. Different techniques are available each having some plus points and some drawbacks.

B. IMAGE STEGANOGRAPHY TECHNIQUES

While going through different types of steganography previously it was seen that there is not only one but several ways to perform any certain type of steganography whether it be text, audio, image or video Steganography. Each technique has its own advantages and drawbacks. Here we will discuss the different image steganography techniques that can be used to hide information within digital images.

I. Least significant bit (LSB) technique
II. ADT (Adaptive Threshold technique):
III. Replacing Moderate significant Bit technique.

X. REVIEW OF LITERATURE

Steganography and cryptography both are Greek terms; steganography means “covered writing” whereas cryptography means “secret writing”. Cryptography deals with hiding information and Steganography deals with composing hidden messages in such a way that only the sender and receiver know about the existence of the message. Whereas in cryptography the existence of the secret message is visible to the whole world because the outer looks of the message are changed which are clearly visible to human eye. The system is broken in cryptography when the attacker can read the secret message. And in Steganography breaking the system first requires the attacker to detect that Steganography has been used. We can achieve more secure systems when we combine both cryptography and steganography, one way is to first hide the message using cryptography and the cover it using Steganography, hence in this way sending the data will be more secure and the possible to attackers to detect it will be minimized.

VIII. METHODOLOGY

Image steganography is being done through image processing. Image processing is used to convert an image into coded text.

XI. RESULT

With all the discussion that has been done above, we can conclude our idea on two parts that is hiding the data within the image and then extracting it later.

A. Hiding Information

Step 1- Load the application

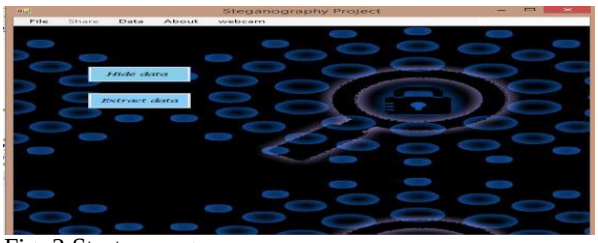

Fig. 2 Startup page

Initially when a user loads the application he will have two options. To hide data we will first click on the „hide data" button.
Now the window will look like this:

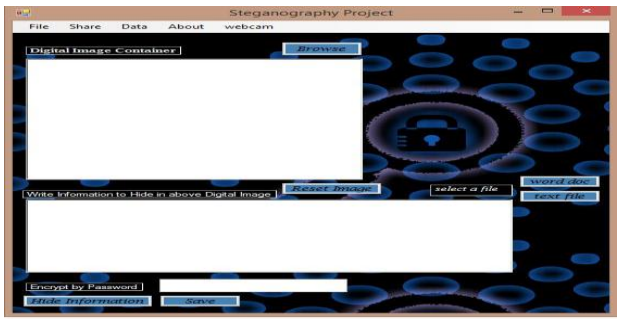

Fig.3 loaded form

Step 2-Load an Image

To load an image from the computer we will click on the browse button. And then a window will appear helping us to select our desired image.

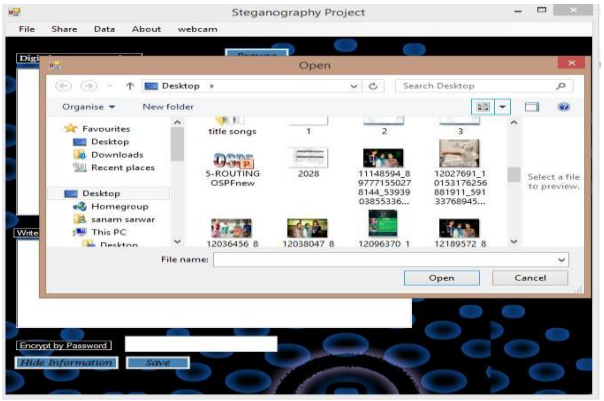

Fig.4 browsing image

Step 3-Load a file

Now when the image is loaded the user can either enter direct text or can upload a text/word File by selecting any one of the options.

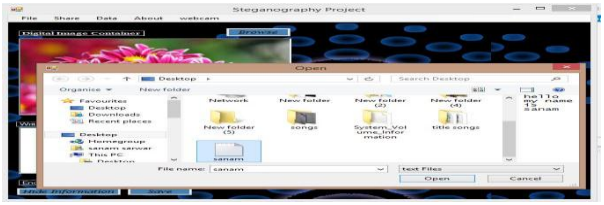

Fig.5 loading a file

Step 4- Hide the information

Hide the information by simply clicking the hide information button. After that save the stegno image to any destination by pressing save button.

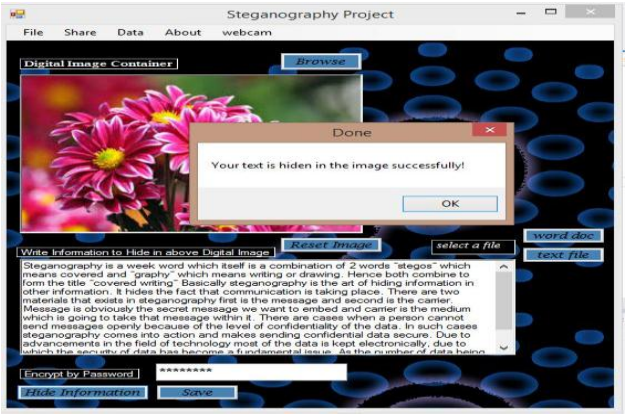

Fig.6 hiding the information

Saving the image:

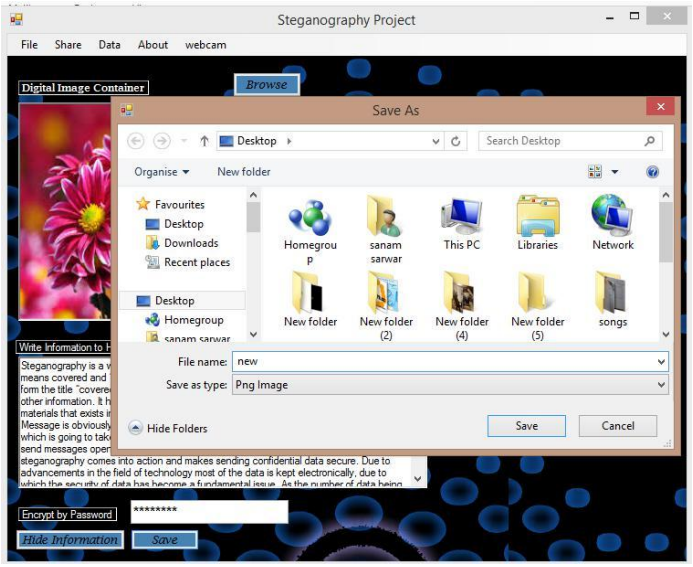

Fig.7 Saving the image

The image in this case has been saved with the name "new.png" on the desktop.

X. EXTRACTING INFORMATION

The process of extraction is just the reverse of the above procedure.

Step1- Mark the Extract Information menu bar

When you want to extract the information go the "data" menu, under it check the extract data button which was previously unchecked

Fig.8 Extract menu bar

Step2- Selecting the Image

Now browse for the image which has the secret information within it.

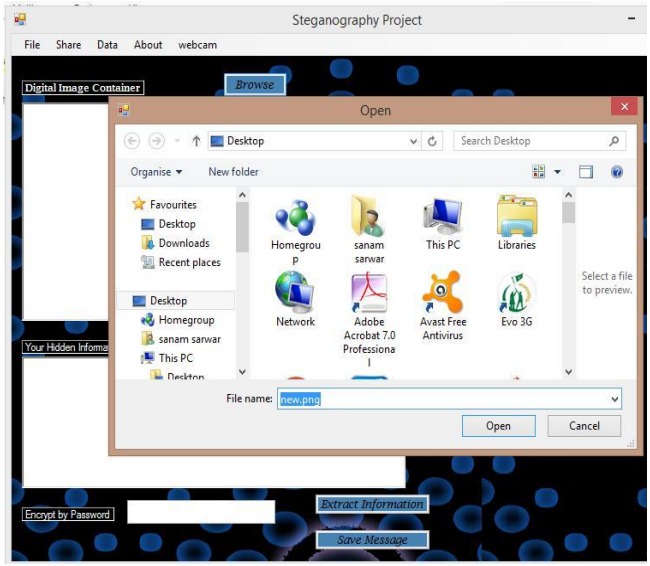

Fig.9 Image selection

Step3- Enter Password

Now enter the password which you previously entered while hiding the data.

Fig.10 Enter password

Now click the extract information button and you will get your secret message.

Fig.11 Extracted Data

XI. TRANSMITTING THE IMAGE OVER INTERNET

Once we have encrypted the information within the image then we can directly send that image to anyone over the internet using Facebook, yahoo, Hotmail etc. on the "share" option in the menu bar there are various options. For example if the user clicks on Facebook then browser will directly open Facebook from your application.

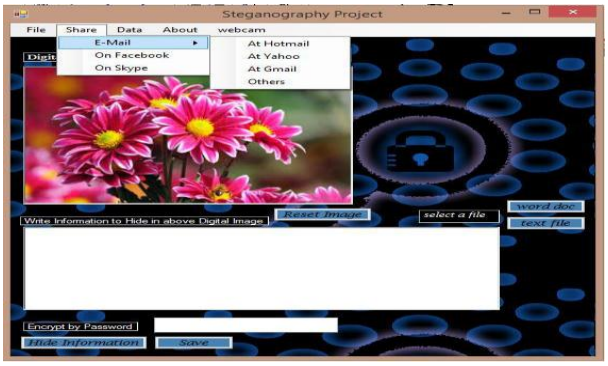

Fig.12 transmitting option

XII. CONCLUSION

It was a detailed Paper "Hiding information within images using steganography". We hope this report fulfilled the requirements for which it was built. We hope this project will be a new step in the field or internet security and with the help of this we can make transmitting data more secure. Currently we are dealing with simple plain text files and word documents or immediate text but this application can be extend for PDF document and such formats. As today social media is an active part of every one's life so if we implement this application for mobile phones so encryption can be possible for messages (but the information should be small or few words, because people do not use large text in SMS), and image steganography can consider WHATSAPP and FACEBOOK parameters.

REFERENCES

[1] http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.208.5 195

[2]http://www.jatit.org/volumes/Vol36No1/1Vol36No1.pdf

[3] http://www.aaronmiller.in/thesis/

[4] http://group50project.blogspot.co.uk/

[5]]http://www.ivanexpert.com/blog/2010/05/the-5-types-of-digital-image-files-tiff-jpeg-gif-png-and-raw-image-files-and-when-to-use-each-o/