INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

HIDING DATA WITH IN DATA

M.Sahithi
B-Tech Student

B.Chandini Sri
B-Tech Student

E.Keerthi Kumar
B-Tech Student

Dr. V. Malsoru
Professor

Department of Information Technology
CMR Technical Campus
Kadlakoya (V), Medchal, Hyderabad-501401

Abstract: In today’s dynamic and information rich environment, information systems have become vital for any organization to survive. With the increase in the dependence of the organization on the information system, there exists an opportunity for the competitive organizations and disruptive forces to gain access to other organizations information system. This hostile environment makes information systems security issues critical to an organization. Current information security literature either focuses on unreliable information bydescribing the information security attacks taking place in the world or it comprises of the technical literature describing the types of security threats and the possible security systems. The system deals with security during transmission of data. Commonly used technologies are Cryptography. This system deals with implementing security using Steganography. In this the end user identifies an image, which is going to act as the carrier of data. The data file is also selected and then to achieve greater speed of transmission the data file and image file are compressed and sent. Prior to this the data is embedded into the image and then sent.

I. INTRODUCTION

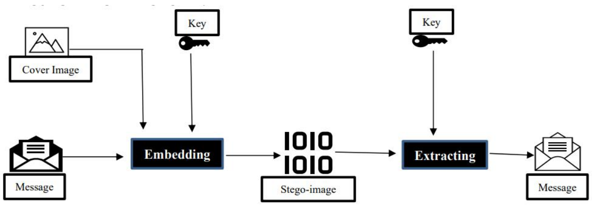
The growing use of Internet needs to take attention while we send and receive personal information in a secured manner. For this, there are many approaches that can transfer the data into different forms so that their resultant data can be understood if it can be returned back into its original form. This technique is known as encryption. However, a major disadvantage of this method is that the existence of data is not hidden. If someone gives enough time then the unreadable encrypted data may be converted into its original form. A solution to this problem has already been achieved by using a “steganography” technique to hide data in a cover media so that other cannot notice it. The characteristics of the cover media depends on the amount of data that can be hidden, the perceptibility of the message and its robustness. In this document, I propose a new system for hiding data stands on many methods and algorithms for image hiding where I store on data file, called sink file in an image file called as container image. The primary objective is to use steganography techniques so as to provide more security and simultaneously using less storage. In this project, we propose to develop a system to hiding data by using "STEGANOGRAPHY" technique as I used many methods stands on some techniques to have at the back-end software for hiding data based on hiding algorithms. After studying the data hiding algorithms we found many ways to hiding data by using the multimedia files and the main question for me was "Where hidden data hides?" as we found by our search to know where the data hides it's important to know what is the file type of the data that it shall be hidden and the cover file type so it is possible to alter graphic or sound files slightly without losing their overall viability for the viewer and listener. With audio, you can use bits of file that contain sound not audible to the human ear. With graphic images, you can remove redundant bits of color from the image and still produce a picture that looks intact to human eye and is difficult to discern from its original. It is in those bits that stego hides its data. By the final of our research we developed a software uses an algorithm, to embed data in an image; The purposed system is called "Steganography", the aim of this project is to encrypt the data; the meaning of encrypt is to hide the data over an image using different steganographic algorithms, in this system LSB is the algorithms that we use to hiding the data. Existing system: The basic principle is this: A message being sent is known as plaintext. The message is then coded using a Cryptographic Algorithm. This process is called Encryption, an Encrypted message is known as Cipher Text, and is turned back into plaintext by the process of decryption. Encryption can be done using Symmetric or Asymmetric Algorithms. In Symmetric algorithms, only one key is used both to encrypt and decrypt the message. In Asymmetric Algorithms, a key used to encrypt a message is different from the key that is used to decrypt the message. There are several algorithms present in the market for Cryptography.Some of the commonly used once are IDEA and RSA that involves Asymmetric or Symmetric methods and also involves private and public keys. **Proposed System:** The algorithms present in the existing system were somewhat complicated. In Cryptography, the meaning of data has been changed. So, it makes intention to the hacker to hack or destroy the data. In our proposed system, we implement a new technology called Steganography for Network security. It not only changes the meaning of data but also hides the presence of data from the hackers.

II. LITERATURE REVIEW

Two interesting examples of steganographic applications were presented in the media in early in August 2011: one of these applications as a potential benefit, and another a potential threat. The two applications were named “Telex” and “Stegobot.” In the first case, researchers at the University of Michigan used steganography to bypass censorship by hiding redirection information in a message to a non-blocked website, which would forward the transmission to a blocked website [Krebs, 2011]. In the second case, researchers from the University of Illinois at Urbana–Champaign and the Indraprastha Institute of Information Technology in New Delhi, India, designed a proofof-concept botnet that used the popular Facebook website to steal and hide private data in pictures on Facebook [Liebowitz, 2011]. In “A Few Words on Secret Writing,” Edgar Allan Poe [1841] writes, “As we can scarcely imagine a time when there did not exist a necessity, or at least a desire, of transmitting information from one individual to another, in such manner as to elude general comprehension; so we may well suppose the practice of writing in cipher to be of great antiquity.” Throughout history, protecting information has been a vital function in many contexts. Although cryptography the transformation of messages so they can be decoded only by recipients who have the decryption key—has received a great deal of attention in the era of computers, other methods of securing information exist that may be just as important. One of these is steganography, the study of hiding messages and other data. Literally meaning “covered writing,” steganography can often pass through checks that would intercept encrypted messages due to their suspicious appearance. Cryptographically altered messages typically appear unrecognizable and raise suspicion, but the “cover” in steganography does not attract attention to senders, messengers, and recipients alike [Warkentin et al., 2008]. Essentially, the idea behind steganography is deception and security through obscurity. A hidden message is injected into a “carrier” medium or carrier message. The carrier, and not the hidden message included, appears to be the relevant item. Ideally, the carrier with the hidden content is indistinguishable from the carrier prior to injection, at least it appears so to third parties inspecting it. Of course, some change of the carrier is inevitable after the hidden message has been included. This change in carrier can be used to discover hidden content, and the success of the technique depends on a combination of the ability to hide content and reduction of change in original carriers. If a steganographic technique is successful, attempts to intercept the message should fail to separate innocuous items from items with hidden content by parties not among the intended recipients. Strong steganographic techniques combine high hiding ability with low probability of detection. Many people have used steganography without realizing it. For instance, a simple method of steganography is writing a letter on the back of a photograph, and hiding the message by inserting the photograph into a frame. Even when crossing borders at a government checkpoint, the message would likely pass customs inspectors checking travel documents unless a full search was conducted. In the digital age, steganography can take many forms, including hiding data in image files, multimedia files, and documents. Even the use of computer viruses has been suggested to hide the presence of steganography [Hansmann, 1997]. Basic types of steganography will be discussed later.

III.IMPLEMENTATION

System Architecture



Module description

User Module
That has major controlling of the whole systems process and able to access or use all modules of the application.

System Module
The Application itself which can perform the user operation in main process encrypt (hide image in another image), decrypt (unhide image from Stego-image).

Least Significant Algorithm The use of multimedia digital signal has become very popular in the last decade due to the spread of wireless Internet-based services such as introduction of the fourth-generation mobile communication systems, user can transfer data up to 1Gbps .Due to the availability of low cost editing tools, digital data can be easily copied, modified and retransmitted in the network by any user. To effectively support the growth of multimedia communications, it is essential to develop tools that protect and authenticate digital information. In this contribution, we present a novel embedding scheme based on the LSB technique. If the value of the pixel of an image is changed by a value of '1' it does not affect the appearance of the image. This idea helps us to for hiding data in an image.In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. If anyone have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image.. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today.

IV.RESULT

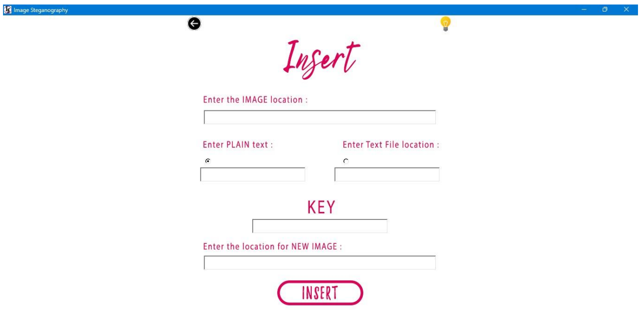
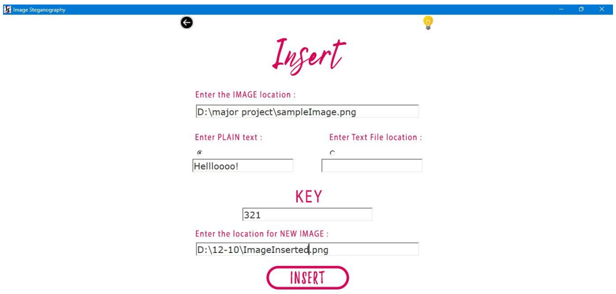


Image Steganography
Insert
Enter the IMAGE location :
Enter PLAIN text :
Enter Text File location :
KEY
Enter the location for NEW IMAGE :
INSERT

Fig-7.2: Insert text
The Screenshot 7.2 is the window where the user1 enters the insertion details.



Enter the IMAGE location : D:\major project\sampleImage.png

● Enter PLAIN text : Hellloooo!

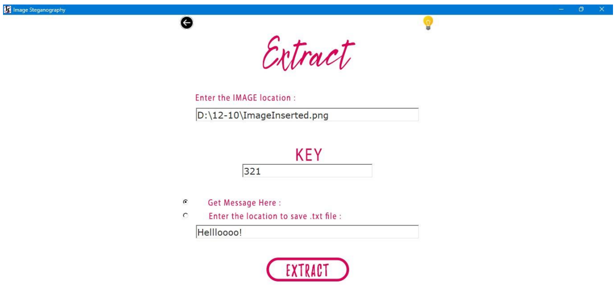
○ Enter Text File location :

KEY 321

Enter the location for NEW IMAGE : D:\12-10\ImageInserted.png

Fig-7.4 inserting the text directly

Here the Screenshot 7.4, the location of the existing image is given first and then the message that must be hidden is given directly as a plain text by choosing “Enter PLAIN text” option. Key to open the text is given as “321”. Lastly the location is provided in order to place the image with the encrypted key in a new location.



Enter the IMAGE location : D:\12-10\ImageInserted.png

KEY 321

● Get Message Here :
○ Enter the location to save .txt file :

Hellloooo!

Fig-7.6: Extracting the text directly

Here in Screenshot 7.6, when the other end user enters the new location of the image along with the key the message displays in the same window, as he has chosen “Get Message Here”.

V. CONCLUSION

Although only some of the main image steganographic techniques were discussed in this document, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden. The proposed approach in this project uses a new steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded inside the cover file image. Used the Least Significant Bit algorithm in this project for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithms.

REFERENCES

1. Rosziati Ibrahim and Teoh Suk Kuan, Steganography Imaging System (SIS): Hiding Secret Messageinside an Image
2. http://www.iaeng.org/publication/wcecs2010/wcecs2010_pp144-148.pdf
3. zaidoonkh. al-ani, a.a.zaidan, b.b.zaidan and hamdan.o.alanazi, overview: main fundamentals for steganography http://arxiv.org/ftp/arxiv/papers/1003/1003.4086.pdfBereSachinSukhadeo, User Aware Image Tag Refinement
4. http://www.ijcsmr.org/eetecme2013/paper19.pdf
5. Youssef Bassil , A Simulation Model for the Waterfall Software Development Life Cycle, 2011 http://arxiv.org/ftp/arxiv/papers/1205/1205.6904.pdf
6. analysis model waterfall model
7. http://www.scribd.com/doc/87322736/Analysis-Model-Waterfall-Model
8. B. Beizer, Black Box Testing. New York: John Wiley & Sons, Inc., 1995. A. Bertolino, "Chapter 5: Software Testing," in IEEE SWEBOK Trial Version 1.00, May 2001.
9. Testing Overview and Black-Box Testing Techniques
10. http://agile.csc.ncsu.edu/SEMaterials/BlackBox.pdf
11. Jovanović, Irena , Software Testing Methods and Techniques,
12. http://www.internetjournals.net/journals/tir/2009/January/Paper%2006.pdf
13. Hong Cai1 and SosS.Agaian2, breaking f5 in color images with low embedding rates
14. Yao Wang, DCT and Transform Coding
15. N. F. Johanson and S.Jajodia. “Exploring Steganography: Seeing The Unseen,” IEEE CJ, February 1998, pp. 26-43.
16. L.Y.Poretal.,“StegCure:A Comprehensive Steganographic Tool Using Enhanced LSB Scheme,” WSEAS Transactions on Computers, vol. 7, no. 8, August 2008, pp. 1309-1318.