RESEARCH ARTICLE OPEN ACCESS

Image Steganography Using Optimal Random Substitution

Satwant Singh[1], Proff. Lekha Bhambhu[2]
Research Scholar[1], Head of the Department[2]
Department of Computer Science and Engineering
JCDMCOE, Barnala Rd, Sirsa
Haryana - India

ABSTRACT
Image Steganography is the art of hiding data into image. As the Internet has become so popular that keeping security through the online communication becomes a matter of concern. Various techniques are developed for the secure communication between two parties. In this research an old technique which is widely used named LSB is used but in some different manner. In this the optimally random pixel is chosen for hiding the secret information into the image. Some results are also shown in this paper which will show that there is no change in the quality of the image. Our main aim in this is to provide more security and develop a technique through which steganography can be achieved with in less time.
Keywords:- Image, MATLAB

I. INTRODUCTION

Steganography is the art and science of hiding data in such a way that only receiver of that message can detect the message. Encryption means to encode .The important of reducing a chance of the Information being detected during the transmission is being an issue now days. Some techniques and solutions are discussed that how to pass information so that the attacker cannot detect.

In this project we will use the steganography method to encrypt the data. [2]Steganography comes from Greek and literally means, "Covered writing". Steganography is closely related to hidden channel scheme. It is the art and science of writing of hidden message in such a way that no one apart of intended recipients knows the existence of message. it is fair to say that steganalysis is both an art and science. The art steganalysis plays a major role in the selection of features or characteristics to test for hidden message, while science helps in designing the text message themselves. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The main difference between these is that in steganography the changes are not visible but in cryptography changes are visible so that it can draw attention and moreover cryptography scrambles a message so it cannot be understood but steganography hides the message so it cannot be seen.

A message in cipher text might create a doubt on the part of recipient while an invisible message created with steganography methods will not. Since steganography is used to hide the occurrence of communication, it has been applied to covert communication, watermarking and fingerprinting that seems to hold the promise for copyright protection, tracing source of illegal copies. Aiming at detecting secret information hidden in a given image using steganography tool, steganalysis has been interest since the end of 1990's.

Various techniques used in steganography:

A). Spatial Domain Embedding

Spatial domain embedding technique first proposed in the literature [5]. Generally, these technique operate on the principle of tuning the parameters of cover image (e.g., the payload or disturbance) so that difference between cover image and the stage-images little and imperceptible to the human eyes. Their popularity derived from their simple algorithmic nature and ease of mathematical analysis spatial domain embedding is easy to implement, providing high pay load capacity but their robustness is weaker than their counterpart. The most widely known image based algorithm is based on modifying the least significant bit layers of image hence known as the LSB technique.LSB based methods can be divided into two main groups: LSB replacement and LSB matching. In LSB replacement, the LSB bit of cover image is replaced with secret bits. While in LSB matching, pixels are randomly incremented or decremented by secret bits.

B). Transform Domain Embedding

As given in literature[6] Transform domain embedding includes discrete Fourier transform (DFT), discrete cosine transforms (DCT), and discrete wavelet transforms (DWT). Regardless of the domain significant transform coefficients are often selected to mix with secret signal in a way such that information hiding transparent to human eyes. These transforms may be applied block wise, or over the entire image. For the block wise transform the image is broken into smaller blocks (8*8 and 16*16 are two popular sizes), and the transform steganography is performed individually on each block.DCT domain embedding technique is most popular one Mostly because of the fact that DCT based image format are widely available in public domain as

well as the common output format of digital cameras. Embedding in DCT domain is simply done by altering the DCT coefficients.DWT domain based embedding technique is quite new, and not as well developed or analysed as technique which operate on DCT or DFT. But such technique will gain popularity asJPEG2000 compression becomes more popular. Stego as per embedding technique based on wavelet operates on JPEG2000images. Embedding is done by modifying least significant bits of selected wavelet coefficients.
, which aims to make communication unintelligible to those who don't possess the right keys. Once a third party can reliably identify which images contain secret messages, the stenographic tool becomes useless. Another important factor is the choice of the cover image. The selection is at the discretion of the person who sends the message. Images with a low number of colours, computer art, and images with unique semantic content should be avoided as cover images.

Problem Formulation

In today's world security is the major issue in communication. When data is send over a wireless network there are chances of hacking/stealing the data. As already some protocols, techniques are existing on the internet, which is given below:

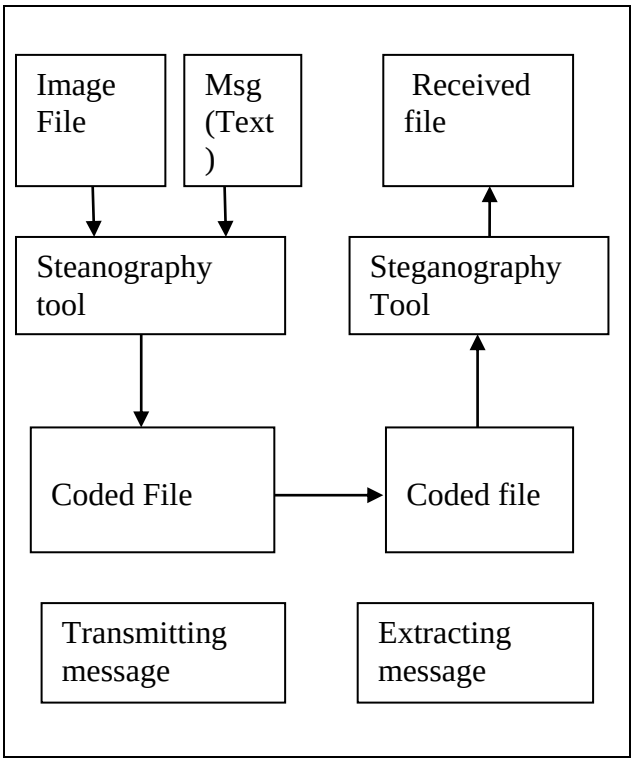
1) Sniffing
2) Spoofing

SNIFFING

Sniffing is the process of spying on the internet. A sniffer is a program that intercepts and decodes network traffic broadcast through a medium. Sniffing is the operation by a machine that it is copies contents of a network packet sent by some other machine to some another one. Such type of sniffing is not a TCP/IP problem, but it is enabled by the choice of broadcast media, Ethernet and 802.11, as the physical and data link layers. It is simpler to sniff wireless networks than wired ones. It is easy to sniff the wireless traffic of a building by locating the equipment at a distance of mile. In a wired network, the attacker must find a way to set up the sniffer on one or more of the hosts in the addressed subnet.

SPOOFING

Spoofing is the well-known technique exist on the both wired and wireless networks. In the case spoofing network attacker constitute frames by marking selected fields that contain addresses or identifiers with recognized looking but non-existent values, or with values that belong to others. The attacker may collect these accepted values through sniffing. A larger number of spoofing techniques is available in the computer world, for example MAC Address spoofing etc., which may result in loss of the important data.
These techniques are well developed in today's world and everyone is aware of these exiting techniques. So, there are more chances of stealing or hacking the information during the transmission. To protect our information from stealing/hacking here is a technique named as Steganography which is proposed in our dissertation work. We, work on this



technique in our dissertation work using MATLAB platform. This will be a new technique which will help in a better data hiding, providing more security to the information from various threats as hacker's crowd is not aware about this new technique.

II. METHODOLOGY

The proposed methodology used in this research is show in this paragraph. In the digital steganography, data is first encrypted by the usual means and then inserted, using a special algorithm into redundant (that is, provided but unneeded) data that is part of a particular file format such as a JPEG image. Think of all the bits that represent the same colour pixels repeated in a row. By applying the encrypted data to this redundant data in some random or no conspicuous way, the result will be data that appears to have the "noise" patterns of regular, no encrypted data.

Steps used in this Algorithm are
Begin
1. Message Text
2. Image file
3. Steganography tool: LSB using optimal random substitution
4. coded file or stego image
5. Transmission
6. Extracting message
7. Decoding
8. Secret message generation
9. Original image
End

III. EXPERIMENTAL RESULTS

Image without steganography

(i) CHELSEA size-19.8kb

Image after steganography

(ii)CHELSEA size-19.7kb

Image without Steganography

(i)Little girl size-32.4kb

Image after steganography

(ii) Little girl size-34.6kb

IV. CONCLUSION & FUTURE WORK

.Various techniques are developed for the secure communication between two parties. In this research a old technique which is widely used named LSB is used but in some different manner. In this the optimally random pixel is chosen for hiding the secret information into the image. Some results are also shown in this paper which will show that there is no change in the quality of the image. Our main aim in this is to provide more security and develop a technique through which steganography can be achieved with in less time. Various future work is to be done in this such as to increase more security the double steganography can be done or the other way is to firstly encrypt the message using the best cryptography algorithm then use the steganography. Both steganography and cryptography can be used as this is the another topic for research.

V. REFERENCES

[1] Hide and seek: An introduction to steganography, 1540-7993, 2003 IEEE security and privacy.

[2] SANS institute infosec reading room :steganography : past, present ,future

[3] Miroslav Dobsicek :Modern Steagnography

[4] Yambem Jina Chanu, Themrichon Tuithung, Kh. Manglem Singh "short survey on image steganography and steganalysis techniques" ,978-1-4577-0748-3/ 2012 IEEE.

[5] Ge Huayong , Huang Mingsheng, Wang Qian, "Steganography and steganalysis based on digital images "978-1-4244-9306-7 2011IEEE conference on image and signal processing.

[6] Vijay Kumar, Dinesh Kumar, "Performance evaluation of DWT based image steganography" 223-228 , 2010 IEEE 2nd international advance computing conference .

[7] R.Amrittharajan, Sandeep kumar behera, Abhilash Swarup,"Colour guided colour image steganography " universal journal of computer science and engineering technology 16-23,oct. 2010

[8] Prabakran.G, Bhavani.R " A modified secure digital image steganography based on discrete wavelet transform", 1096-1100, 2012 IEEE

[9] Chi-Kwong Chan∗, L.M. Cheng "Hiding data in image by simple LSb substitution", the journal of the pattern recognition society, pattern recognition 37(2004) 469-474.

[10] R.Amritharajan, r.akila, P.Deepika chowda varapu,"A comparative analysis of image Steganography" international journal of computable applications (0975-8887) ,volume 2-No.3,May-2010.

[11] W.Bender,D.Garhul,N.Morimoto,A.Lu," Techniques for data hiding" IBM System journal VOL.35,NOS 3&4,1996.