Data Hiding using LSB Substitution

Randeepika Samagh[1], Shailja Kumari[2]

Research Scholar[1], Lecturer[2]
Department of Computer Science and Applications, C.D.L.U, Sirsa
Haryana - India
nitisamagh87@gmail.com

ABSTRACT

Image Steganography is the art of hiding data into image. 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, Steganography, LSB, Pixel.

1. 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. 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.

1.2 WHAT IS DIGITAL IMAGE???

Digital image is the 2D array of m*n pixels. In the image processing the digital image refers to the colors that is white and black

F(x, y)

Image is represented by the function f(x, y) where x and y are the ordinates of the pixel and F is the brightness of the point (x, y). the pixel represents the value of the x & y and the co ordinate (0,0) is located at the top, left corner of the image. The value of x increases moving from left to right, and the value of y increases from top to bottom. In digital image processing, an imaging sensor converts an image into a discrete number of pixels. The imaging sensor assigns to each pixel a numeric location and a gray level or color value that specifies the brightness or color of the pixel.

Image is made up of lots of little dots called pixels. Each pixel has 3bytes. One byte for Red, one for Green and one for Blue.

Difference between 2 colors that differ by one bit in either one red, green or blue value is impossible to detect for a human eye. So we can replace LSB in a byte, we can either add/ subtract one or more values from the value it represents means we can overwrite last bit in a byte without affecting the color it appears to be and resulting a minor distortion.

1.3 PROPERTIES OF THE DIGITAL IMAGE:

- **IMAGE RESOLUTION**

The number of rows and columns of the image are called the resolution. An image made of m columns and n rows has a resolution of m x n. this image has m pixels along its horizontal axis and n pixels along its vertical axis.

- **IMAGE DEFINITION**

The number of shades that one can see is called the image definition. The bit depth of an image is the number of bits used to encode the value of a pixel. For a given bit depth of n, the image has a image definition of 2^n , meaning a pixel can have 2^n different values. For example, if n equals 8 bits, a pixel can have 256 different values ranging 0 to 255. If n equals 16 bits, a pixel can have 65,536 different values ranging 0 to 65,536 or from -32,768 to 32767.

1.4 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:**

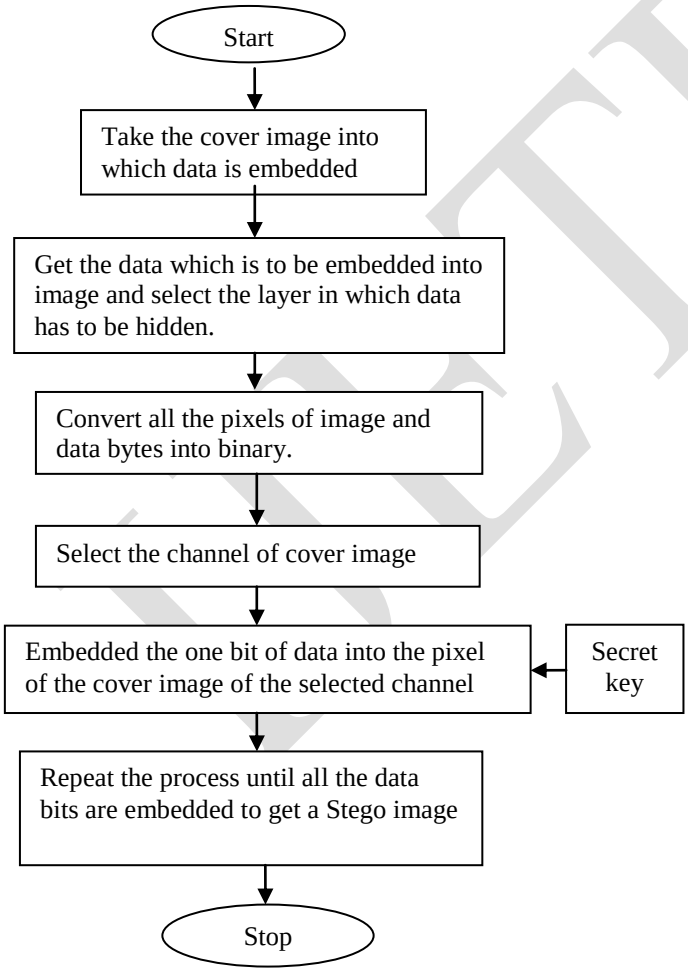
Sniffing is the process of spying on the internet. A sniffer is a program that intercepts and decodes network traffic broadcast through a medium. Sniffing is the operation by a machine that it copies contents of a network packet sent by some other machine to some another one. Such type of sniffing is 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 that exists 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.

2. METHODOLOGY

The proposed methodology used in this research is show in this paragraph. It is done by implementing the following steps in a sequential manner:



- Select the image which will be used to embed data.
- Then convert the data into character format which will be embedded into image.
- Then we will select the 1 Dimensional image only that is RGB
- Convert all the pixels of image and data bytes into binary.
- Select the green and blue channel of the cover image.

- Then embed each bit into each pixel of the image into the channel which is selected
- Repeat the process until all the data bits are embedded to get a Stego image.
  In the end we will get the Stego image which will look similar to the original image. Now the data is hidden into that image. In the same way the reverse process is used to extract the message that is hidden into the image. But for that we need the key that is used in the algorithm. The algorithm designed and processed in Matlab platform.

3. RESULTS

Normal Image

Stego Image

From the results we conclude that it is a very hard task to find out any resemblance between the Stego image and cover image. So, it is very difficult for the steganalyst to find out the secret data. That means the designed algorithm provides a security of secret data (hidden data) up to 99.9%. The size of images are also almost similar. The main work done in this project is that the time taken by this algorithm is very less.

4. 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.

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.
[12] N. Akhtar, ; P. Johri, ; S Khan, ―Enhancing the Security and Quality of LSB Based Image Steganography‖ 5th International Conference on Computational Intelligence and Communication Networks (CICN), Publication Year: 2013, Page(s): 385 – 390
[13] R.P Kumar, V. Hemanth, M ―Securing Information Using Sterganoraphy ‖ International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013, Page(s): 1197 - 1200

AUTHORS

Miss. Randeepika Samagh is presently doing M.Tech (CSE) from C.D.L.U as a part-time student and working as School Information Manager (SIM) in Govt. Sr. Sec. School, Sirsa. Now-a days just dedicated to her Thesis work. She had done B.Tech in IT in 2009 from J.C.D.M.C.O.E, Sirsa. she has $2^{1/2}$ years of academic experience and $2^{1/2}$ years of administrative experience.