Volume: 2 Issue: VII Month of publication: July 2014

DOI:

www.ijraset.com Vol. 2 Issue VII, July 2014

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Securing Data in Fiber Optics

Ms. Babita Rawat[1], Mr. Mukesh Sone[2]

1. M.Tech. Student (Electronics & Communication), Invertis University, Bareilly, U.P., India
2. Associate Professor, Deptt. of Electronics & Communication, Invertis University, Bareilly, U.P.,India

Abstract- Fiber optic has previously displayed unbeaten advantages, and was the most secure communication medium, but now it is very easy to tap fiber optic networks. There are a number of known methods of extracting or injecting information into a fiber, while avoiding its detection. Therefore it has become necessary to secure data in optical fiber.

This paper provides securing data flowing in optical fiber through steganography. Steganography is a process that involves hiding a message in a carrier, then the carrier is sent to receiver without anyone else knowing that it contains a hidden message. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. Then at the receiver original data is extracted from received data. This paper provides an overview of steganography and steganographic technique to secure data i.e. both image and text.

Keywords: Optical Fiber Tapping, steganography, cryptography, stego, steganlysis.

I. INTRODUCTION

Fiber optic cable is the transmission medium of the future. They are gaining popularity for transmitting data as they offer high data transmission rates and are thus particularly suited for the transmission of data, images and voice. The significant advantages of fiber optics are its speed, capacity, economy which has increased its demand dramatically.

Fiber optic seems to be secure when compared with the copper wire but with the advancement in science and technology it has become very easy to tap into fiber optic networks [1], [2]. There are various methods, so-called “Optical Tapping Methods”, to extract data from fiber optic networks [2]. The risk of being detected is very slight, if not non-existent. Anybody looking for the necessary tools can find them easily on the internet. The majority of telecommunications providers, however, fails to draw attention to this growing danger or is blatantly ignorant of the fact [1].According to numerous studies; tapping has multiplied tenfold in the past two years in companies around the globe. The commercial damage resulting from attacks is enormous.

In this we have proposed LSB steganography technique to secure the data i.e. both text and images in fiber and have also implemented it.

II. SECURITY MATTER: TAPPING

Tapping is the process in which data is extracted or injected in the fiber in order to hack into the sensitive information. It can be done by either cutting the fiber to the core or simply bending it. Tapping on fiber optic cables is very simple than was previously thought. It is very hard to detect it but very easy to do it. In this paper steganography technique has been used to secure data in fiber optic cable.

III. PROTECTION TILL NOW

Protection against tapping can be done through cable surveillance and monitoring signals i.e. monitoring signals can be send around fiber such that any attempt to bend the fiber will raise the alarm or we can integrate electrical conductors into fiber cable such that when cable is tampered it will raise the alarm [3]. Fiber cable can also be monitored with optical time domain reflectometer if tapping is detected within the fiber trace. Pilot tone method can also be used to detect transmission disruptions [3], [4]. Encryption can also be done to secure data in fiber optics [5].Each method has strengths and weaknesses with respect to the attack methods, and none can provide full protection.

It is very difficult to monitor the entire fiber optics infrastructure, so data steganography can be the answer to prevent tapping

IV. STEGANOGRAPHY

Steganography is the science of hiding information. In steganography information can be hidden in carriers such as images, audio files, text files, and video and data transmissions. When message is hidden in the carrier a stego carrier is formed for example a stego-image. Steganography hides the message so that there is no knowledge of the existence of the message in the first place. Steganography includes the hiding of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Steganography today, however, is significantly more sophisticated, allowing a user to hide large amounts of information within image and audio files. In this paper both image steganography and text steganography is used for securing images and text respectively.

Text can be hided in an image by replacing some bytes of the image according to the characters of the text. Similarly image can be hided in another image by replacing bits of pixels of second image corresponding to the pixels of the first image matrix.The implementation will only focus on Least Significant Bit (LSB) as one of the steganography techniques as mentioned in below:

A. Hiding Text

An image is the combination of several pixels and each pixel has three color numbers so we can say that there are millions of numbers in an image. In image it works by changing a few pixel color value; Now it will use selected pixel value to represent characters instead of a color value [6].

4.1.1) Process

Firstly the message which has to be hidden is converted into a cipher text i.e. data is converted into the bytes i.e. message is converted into its ASCII equivalent, which then converted into bytes. Now message is embedded into the digital image. In order to hide the message and data is first converted into byte format and stored in a byte array. The message is then encrypted and then embeds each bit into the LSB position of each pixel position. The LSB of each 8bit byte has been cooped to hide a text message. It uses the first pixel to hide the length of message.

Original pixel = (1111101, 01100100, 01100100)
"b" = 01100010(ASCII value 98)
New pixel = (11111011, 01100000, 01100110)
New pixel = (251, 96,101)

4.1.2) *Retrieving Message and Conversion to Text*

Once a message has been retrieved it has to be converted in to the original message. This process can be done by reading the embedded data from the file. The read data will be in bytes format. This can be done by extract the pixels of output image in one array. Decoding will be done in same manner as the reversal of encoding process. After that bytes are converted to text by reading one by one byte to get each character in the message [7].

B. Hiding Image

This process studies an image file as a carrier to hide the original image. Therefore, the carrier will be known as cover-image, while the stego-object known as stego-image. Firstly the cover image and original image is taken. A stego-image is obtained by applying LSB algorithm on both the cover and hidden images. The hidden image is extracted from the stego-image by applying the reverse process.

The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example, suppose one can hide a message in three pixels of an image. Suppose the original 3 pixels are:

(11101010 11101000 11001011)
(01100110 11001010 11101000)
(11001001 00100101 11101001)

A steganographic program could hide the letter "J" which has a position 74 into ASCII character set and have a binary representation "01001010", by altering the channel bits of pixels.

(11101010 11101001 11001010)
(01100110 11001011 11101000)
(11001001 00100100 11101001)

In this case, only four bits needed to be changed to insert the character successfully. The resulting changes that are made to the least significant bits are too small to be recognised by the human eye, so the message is effectively hidden.

V. DESIGN METHODOLOGY

The outcome of this paper is to generate the threshold losses of fiber and a novel approach to create a crossplatform that can effectively hide a message that contains both data files and image files inside a digital image file, if and only if the losses in the fiber increases by its threshold value.

. In this paper the method to secure both data and image inside a digital image through steganography i.e. LSB technique is used to secure the information over the single mode optical fiber is implemented.

The entire operation can be achieved in following steps:

- Data is secured through steganography with the help of matlab software.
- Sending the data.
- Receiving the data.
- Software processing to detect the frames/ packets and extracting desired data from it.

The experiment involves transmitting a data i.e. both text and image over optical Ethernet from one computer to the other. Firstly data is secured through steganography at sender's side computer with the MATLAB software. Then data goes through unidirectional Ethernet media converter so that two dissimilar media types such as twisted pair with fiber optic cabling can connect together. Then at receiver data is received and desired data is extracted through software processing (MATLAB).

Above mentioned hardware and software are connected as shown in figure. The experiment reported here was performed on an Ethernet network as the components especially the software were easily available.

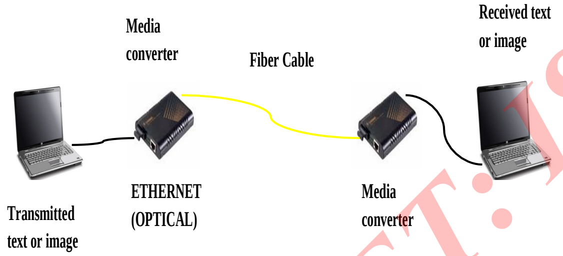

Fig. 5.1 Experimental setup for optical communication

Fiber Tapping is a tactile threat to the interests of national security, financial institutions or even personal privacy and freedoms. Once tapped, the information thus obtained can be used in many difference ways as per eavesdropper's motivations and resourcefulness. In this the concept of securing data through steganography is proved both in terms of software and physical experiment.

VI. RESULTS

A. *Losses Results*

The losses are calculated on the optical fiber kit (ST2501) for 3m fiber cable.

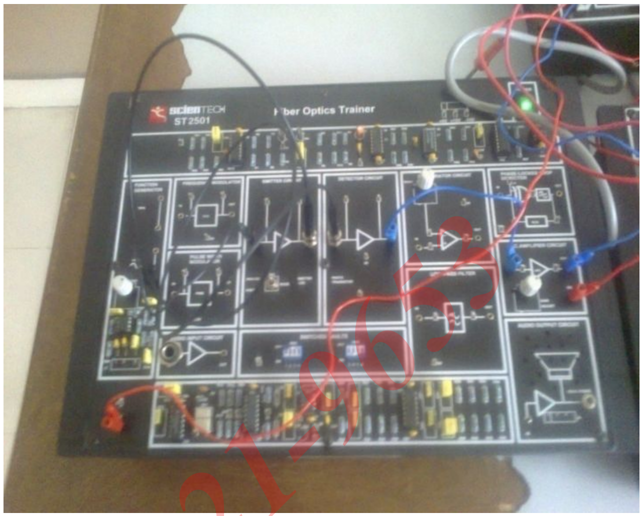

Figure 6.1 Experimental kit

The losses calculated are:

6.1.1 Attenuation Losses

The basic attenuation mechanisms in a fiber are absorption, scattering, and radiative losses of the optical energy. Absorption is related to the fiber material, whereas scattering is associated both with the fiber material and with structural imperfections in the optical waveguide.

It can be calculated as:

$$\alpha(dB)= 10\log(Pin/Po)$$
$$V1/V2=e^{-\alpha\ (L1+L2)}$$

Where:

L1= Short Cable Length
L2=Long Cable Length
α= Attenuation Loss

Maximum value of Attenuation in 9/125 single mode fiber at different wavelengths:

At 1310 nm ≤ 0.40 dB/km
At 1383 nm ≤ 0.40 dB/km
At 1550 nm ≤ 0.25 dB/km
At 1625 nm ≤ 0.25 dB/km

It is concluded that attenuation loss increases as the length of optical fiber increases. It is useful for thesis because there is need of choosing fiber and its length plays an important role. Appropriate length fiber must be chosen for more accurate result.

6.1.2 Bending Loss

Bending is one of the primary causes for increase in attenuation in optical fibers and can be divided in two types,

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

macro and micro bending. For macro bending, the bend radius is much larger than the fiber diameter whereas micro bend looses are caused by more local bending of the fiber.

- Macro bending

The macro bend has a much larger bend diameter than the fiber diameter. Here, the fiber coating has almost no impact on the optical loss as the light is guided in the core, far from the coating. The coating cannot protect the glass (core and cladding) from being bent as the bend diameter is much larger than the fiber.

- Micro bending

The situation is the opposite for micro bending. Here the bending is very local and the coating can protect the glass from external forces applied on the coating surface. For this reasons many fibers has a two layer acrylate coating where the inner layer is soft and can accommodate for external forces acting on the fiber. Fibers with a thin and hard coating such as polyimide do not have this protection from local bending and must be handled more carefully in order to avoid micro bending of the glass.

Macrobending loss r = 7.5 mm,
1 turn 1550 nm =0 db
2 turn 1550nm=0.1db (almost negligible)

This shows that the increase in number of turns increases the bend losses.

6.1.3 Dispersion Loss

Dispersion is the phenomenon in which the phase velocity of a wave depends on its frequency, or equivalently when the group velocity depends on the frequency. An optical signal becomes increasingly distorted as it travels along a fiber.

Chromatic dispersion
1285 - 1330 nm ≤ 3.50 ps/nm × km
1550 nm ≤ 18.0 ps/nm × km

Polarization mode dispersion
For individual fiber ≤ 0.20 ps/√km

It is concluded that when the losses will become greater than these threshold value, then steganography techniques will be applied to the data for securing it.

B. Text Steganography Results

Text to be hidden: “The era of the information revolution is upon us. Bandwidth, performance, reliability, cost efficiency, resiliency, redundancy, and security are some of the demands placed on communications today. Since its initial development, fiber optic systems have the advantage of most of these requirements over copper-based and wireless telecommunications solutions. The largest obstacle preventing most businesses from implementing fiber optic systems was cost. With the recent advancements in fiber optic technology and the ever-growing demand for more bandwidth, the cost of installing and maintaining fiber optic systems has been reduced dramatically”.

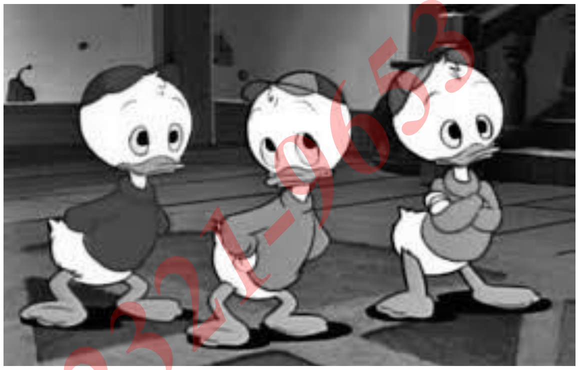

Fig. 6.2 Image in which text will be hidden

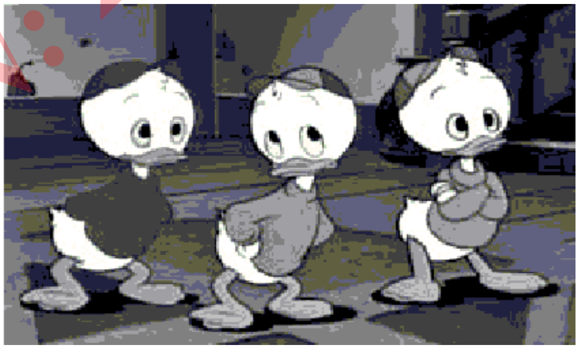

Fig. 6.3 Image after text is hidden

C. Image steganography results

At sender side

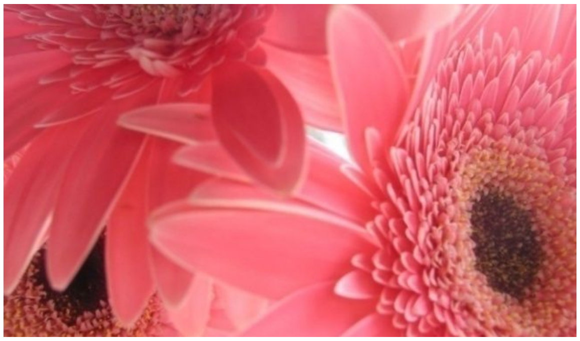

Fig. 6.4 Cover image

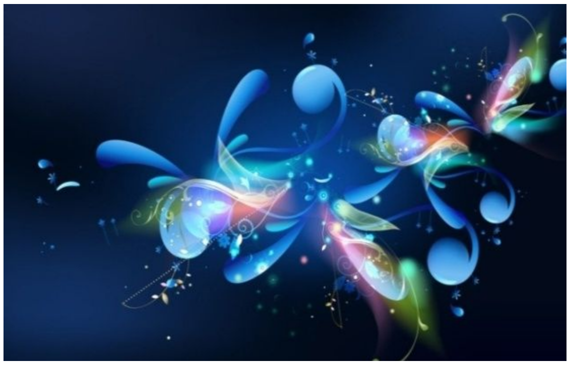

Fig. 6.5 Image to be hidden

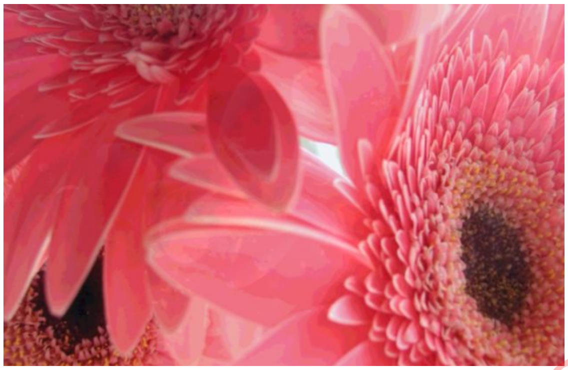

Fig. 6.6 Stego image

Output at receiver's side

At receiver original image is extracted from cover image as shown is figure 6.7

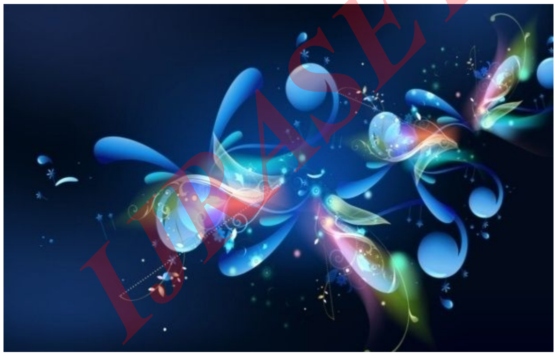

Fig. 6.7 Original image

VI. CONCLUSION

As a communication networks develop, there are many opportunities for businesses to become more streamlined and efficient. However, there are also many more opportunities for unauthorized persons to gain access to sensitive information. The information thus obtained can be used in many difference dangerous ways. If you want to keep prying eyes away from secure data, proper encryption is the most obvious answer. Steganography is a fascinating and effective method of hiding data that has been used throughout history. Methods that can be employed to uncover such devious tactics, but the first step are awareness that such methods even exist. This thesis has proved the concept of securing data through steganography both in terms of software simulation and physical experiment.

REFERENCES

[1] Keith Shaneman & Dr. Stuart Gray; "*Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for detection and Prevention*", IEEE Military Communications Conference 2004.

[2] Arsalan Saeed;*optical fiber security, tapping & its defensive methodologies"*, journal of engg. and sciences 2010.

[3] M Zafar Iqbal, Habib Fathallah, Nezih Belhadj; "*Optical fiber tapping-methods and precautions*", IEEE, 2011.

[4]*http://www.rootsecure.net/content/downloads/pdf/fiber_optic_taps.pdf*

[5] Z. Banjac, V. Orlic, M. Peric, S. Milicevic; "*Securing data on fiber optic transmission lines*", 20th Telecommunications forum TELFOR, IEEE 2012.

[6] Anwar H. Ibrahim, Waleed M. Ibrahim; "*Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time*", nternational Journal of Information Technology & Computer Science (IJITCS) (ISSN No : 2091-1610) Volume 7 : No : 3 : Issue on January / February, 2013.

[7] Saurabh Singh, Gaurav Agarwal: "Use of image to secure text message with the help of LSB replacement", International Journal Of Applied Engineering Research Volume 1, No2, 2010.