Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Securing Data in Fiber Optics through Steganography

Babita Rawat[1]
M.Tech. Student, ECE, IIET,
Invertis University, Bareilly, U.P,
India

Mukesh Kumar Sone[2], **Gaurav Agarwal**[3]
ECE Department, IIET, Invertis
University, Bareilly, U.P,
India

Abstract-Today, the world of business would be inconceivable without fiber optic cables. The main demands of any communication system are speed, security, bandwidth, reliability and cost and all these requirements are fulfilled by fiber optic cables, there is no other means of transporting such huge volumes of information so fast and so reliably. Fiber optic cable has previously displayed unrivalled advantages, and was the most secure communication medium, but now it is very easy to tap into fiber optic networks. There are a number of known methods of extracting or injecting information into a fiber link, while avoiding detection. Therefore it has become necessary to secure data in optical fiber. This paper provides securing data flowing in optical fiber through steganography. It is a method of covertly communicating. Steganography is a process that involves hiding a message in an appropriate carrier for example an image or an audio file, 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 embedded data is extracted from received data. While cryptography provides privacy, steganography is intended to provide secrecy. This paper provides an overview of steganography, general forms of steganography, specific steganographic method and method to secure data i.e. both image and text.

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

I. INTRODUCTION

Today, the world of business would be inconceivable without fiber optic cables. However, what is often forgotten or even denied is the fact that it is very easy to tap into fiber optic networks. The security risk, therefore, should not be underestimated [1]. Fiber optic cables are data communication lines that have previously displayed unrivalled advantages. There is no other means of transporting such huge volumes of information so fast and so reliably. State-of-the-art fiber optic networks are employed by many banks, insurance companies, enterprises and public authorities as the backbone, which just happens to be the place where industrial espionage is child's play. According to numerous, international studies, digital eavesdropping has multiplied tenfold in the past two years in companies around the globe. The commercial damage resulting from attacks of this nature is enormous. Fiber optic cable is the transmission medium of the future. They are gaining increasing popularity for transmitting data with estimates putting the length of cable installed around the globe at more than 300 million kilometers.

The cables offer high data transmission rates and are thus particularly suited for the transmission of data, images and voice. In carrier networks, Gigabit Ethernet is the access technology whilst fiber optics provides the transmission medium. In day-to-day business, the transfer of information and data has become indispensable, and there is no let up in the volumes that are being transmitted. Bandwidths of 1 Gbps or higher are the order of the day for connecting different metropolitan locations (MAN), for networks throughout Switzerland (WAN) as well as for backup and disaster recovery infrastructures (Storage Area Network, SAN). Even large volumes of data can be mirrored and safeguarded at locations far away from their origins. The terror attacks on the World Trade Centre lost no time in bringing home the importance of remote data backups. The significant advantages of fiber optics for networks of this type – speed, capacity, economy have led to a situation where the demand has increased dramatically.

The widespread notion that fiber optic cables are particularly secure when compared with the traditional copper wire is not quite accurate since 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.

This paper presents securing data flowing in optical fiber through steganography. It is a method of covertly communicating. Steganography is a process that involves hiding a message in an appropriate carrier for example an image or an audio file [3]. The carrier can then be sent to a 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. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data. While cryptography provides privacy, steganography is intended to provide secrecy [4]. The paper provides an overview of steganography, general forms of steganography, specific steganographic methods.

© 2014, IJARCSSE All Rights Reserved

II. SECURITY MATTER: TAPPING

Tapping on fiber optic cables is a great deal simpler than was previously thought. It is very easy to determine which fiber optics is being used as the individual cables in a cable loom are marked for maintenance purposes. Thus it is sufficient to identify the cable emerging from a building and tap into it from a freely accessible point. In fiber optic networks several thousand amplifiers can be opened with a square locking key. These amplifiers are equipped with service connectors for maintenance work and thus provide the easiest point of intrusion. The core carries the optical data from the transmitting end to the receiving end and cladding traps the light in the core by using the principal of total internal reflection.
There are various fiber optics tapping, but most fall into the following main categories:

- Fiber bending
- Optical Splitting
- Evanescent Coupling
- V-Groove Cut
- Optical Scattering

2. 1 Fiber Bending

In this method cable is stripped down to the fiber for bending. This method exploits the principle of propagation of light through an optical fiber better described as the total internal reflection. To achieve this, angle of incidence of light on the core cladding interface should be greater than the Critical Angle for total internal reflection. Otherwise some light will radiate out of the fiber through its cladding [5], [6].

2. 2 Optical Splitting

An optical splitter works very much in the same manner as a coax splitter for televisions - it 'splits' a single optical signal into two identical signals. However, in order for the device to be installed, the target fiber must be cut and both ends spliced onto the optical splitter. Once the fibers are accessed within the cable, the splicing of the fibers onto the optical splitter could take as little 2-3 minutes depending on the splicing method used.

2. 3 Evanescent Tapping

The index of refraction (IOR) of fiber core is higher than IOR of cladding. The total internal reflection provides a mechanism to spatially confine optical of the light in one or more selected fiber modes optical guide the optical energy along the fiber core. The guided optical energy in the fiber is not completely confined within the core. In a fiber a portion of the optical energy can leak through the interface between the core and cladding via an evanescent field that essentially decays exponentially with the distance from the core-cladding interface. This evanescent leakage may be used to couple optical energy into or out of the fiber core. Evanescent tapping accomplishes the redirection of a percentage of light into another fiber in such a way that does not require the target fiber to be bent. This is done by polishing the surface of the intentionally exposed target fiber cladding down to a point near the core. The receiving fiber is also polished. This reduced the reflectivity of the victim fibers core causing a percentage of the light to bleed out and into the other fiber. This is essentially what an optical splitter would do but in a less controlled manner [7].

2. 4 V-Groove Cut

In this method, a V-groove is cut in the cladding of the optical fiber close to the core. The V-groove is cut so that the angle between the signal propagating in the fiber and the face of the V-groove is greater than the critical angle for total internal reflection. When this condition is met the fraction of the signal traveling in the cladding and overlapping with the V-groove undergoes total internal reflection and is coupled out through the side of the fiber.
Once again, a precision cut required in the fiber as well as the subsequent polishing would require precision equipment and a great deal of uninterrupted time to install such a tap. However, this method could result in very little optical loss and would be very difficult to detect. Finally, since this process requires actually cutting into (but not breaking) an optical fiber, it is also the riskiest method for achieving a fiber tap in the field.

2. 5 Scattering

The use of a Fiber Bragg Grating to achieve a fiber tap is the most advanced field technique discussed, and also the most difficult to detect via periodic network testing and monitoring. This process requires the use of an Excimer W Laser to create an overlapping and interfering field of W rays that subsequently 'etches' a Bragg Grating onto the fiber core. The grating then reflects a portion of the optical signal out of the target fiber into a capture fiber.

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. 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. 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.

© 2014, IJARCSSE All Rights Reserved

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 [8]. 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 concealment 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 (in which first image is hided) 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:

4. 1 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.

4.1. 1 Text to Byte Conversion

This involves converting the message to be hidden into a cipher text i.e. data is converted into the bytes that are each character in message is converted into its ASCII equivalent, which then converted into bytes.

4.1. 2 Message Embedding In Digital Image

Hiding image involves embedding the message in to the digital image. Each pixel typically has three numbers associated with it, one each for red, green, and blue intensities, and these value often range from 0255. 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 (at spot 0) to hide the length of message (number of character).Suppose last three bits are changed i.e. the bits that determine the “one place”, the “two place” and the “fours place”. We can only alter the original pixel color value by 7.

If we take an example of pixel (225,100,100) with character “a”, then we can obtain:

Original pixel = (11100001, 01100100, 01100100)

“a” = 01100001(ASCII value 97)

New pixel = (11100011, 01100000, 01100101)

New pixel = (227, 96,101)

4.1. 3 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.

4. 2 Hiding Image

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images three bits of information is embed in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden [9]. 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 (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, 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 (24-bit color). 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.

© 2014, IJARCSSE All Rights Reserved

(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 a platform that can effectively hide a message that contains both data files and image files inside a digital image file. 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.

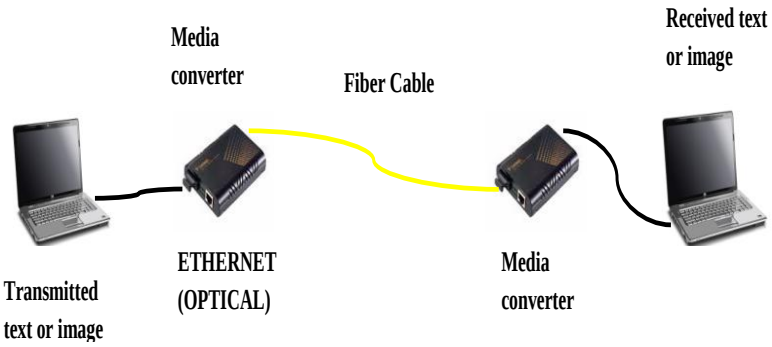

Fig. 5.1 Experimental setup for optical communication

Fiber Tapping is a tangible 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 imaginative 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

6. 1 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".

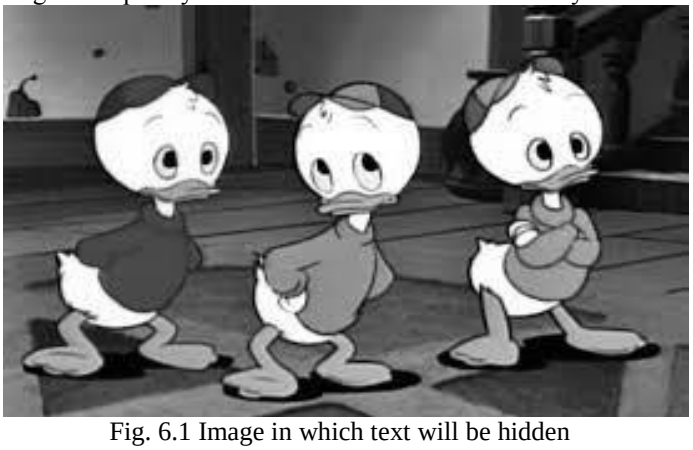

Fig. 6.1 Image in which text will be hidden

© 2014, IJARCSSE All Rights Reserved

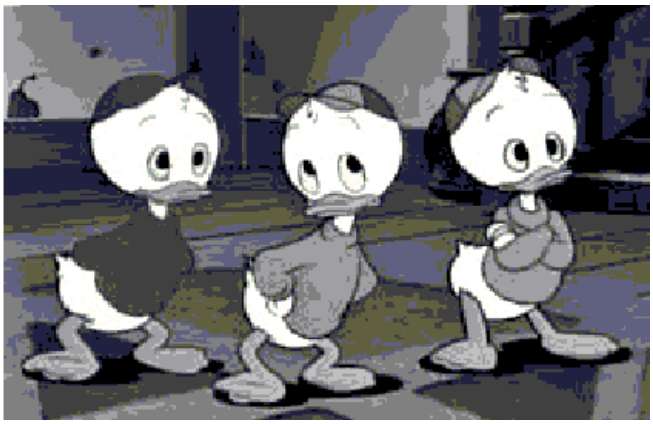

Fig. 6.2 Image after text is hidden

6. 2 Image steganography results

At sender side

Fig. 6.3 Cover image

Fig. 6.4 Image to be hidden

Fig.6.5 Stego image

© 2014, IJARCSSE All Rights Reserved

Output at receiver's side
At receiver original image is extracted from cover image as shown is figure 6.4.

Fig. 6.6 Original image

VII. 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 imaginative ways as per eavesdropper's motivations and resourcefulness. 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] Ronak Doshi, Pratik Jain, Lalit Gupta; "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638 ISSN: 2249-6645.

[4] Rosziati Ibrahim and Teoh Suk Kuan; "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application 2 (2011) 102-108.

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

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

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

[8] 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.

[9] Deepesh Rawat and Vijiya Bhandari; " A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image",International Journal of Computer Applications (0975 – 8887) Volume 64– No.20, February 2013.

© 2014, IJARCSSE All Rights Reserved