Data Security inside Optical Communication Networks through Encoding and Steganography

Wadah Hatim Salim1, Bushra R.Mahdi1, Ayad A. Dhaigham1.

1Ministry of Science and Technology—Materials Research Directorate- Laser and Optoelectronics Research Center, Baghdad, Iraq

Abstract. This paper provides securing flowing of data in optical systems through encoding and steganography. Encoding (Cryptography) and steganography are major elements for secure the data. Suggested communication system aids for transporting huge volumes of information of quickly and reliably. This communication system has previously displayed unrivalled characteristics of most secure. Secure connection requires the integration of cryptography and steganography, so it is very difficult to penetrate it. The system program uses cryptography and steganography to merge any type from files and encrypted text that are effectually hidden for human eye with a carrier image. Also, the extra purpose from this paper is to procure the threshold losses of the optical system and introduce a new approach to create an ideal system that can effectively secrete a message that includes important information, if and only if the optical cable losses increase by its threshold magnitude.

Keywords. Image Processing, Cryptography, Steganography, Optical Fiber Tapping.

1. Introduction

Optical networks security can be effectively protected by optical cryptography and steganography, optical key distribution, including all optical signal processing, fiber-based methods and optical chaos-based communication [1].

Cryptography is a manner of storing and sending information in a specific aspect to intended persons that can read it. The expression is most often correlated with clear text (ordinary text) into encryption text (cipher text), then aback again to decryption. There are different type of cryptography. The first type is symmetric key cryptography in which each of receiver and sender use a single password. The second type is asymmetric key in which each receiver and sender utilizes two passwords: specific password that is affined to being only and general password that is known to anyone. Plenty information cipher algorithms are obtainable and suggested by scholars with differences. The two types of systems are shown in figure (1) and figure (2).Information encryption only might not execute the objective of information safety; cryptography might raise doubt on the part of the attacker and cannot cache the information in the optical system as ideal method [2].
Steganography is the science of hiding data. In steganography data can hide in carriers like text files, video and audio files, images and information transmissions. When message is secreted in the stego carrier is creator for paragon a stego-text file. Steganography secretes the communication so that there is no knowing of the being of the communication in the originally place. Steganography comprises the secretion of data inside system files. In digital electronic and communications steganography may contain steganographic formed with in transmit layer, like document file, image file, program and protocol. Steganography today, is significantly more sophisticated, allowing a user to secrete large amounts of data within audio files and image [3]. Steganography is serviced to full fill high security, robustness and capacity, as shown in figure (3). 1, three traits epitomize a triangle in information obscuring systems that are utilized to decide the system execution [4].

1.1. Least Significant Bit Algorithm
In LSB Algorithm, both the information and the picture to be employed as cover object are transformed from their pixel formula to binary. And the Least Significant Bit of the picture is substituted with the bit of the information to be changed so as to reverse the message that requires to be secreted. The bits of
the information substitute each of the colours of the Least Significant Bit of the picture. Table (1) showing three characters with ASCII values and corresponding binary values [6].

Table 1. ASCII values

| Character | ASCII values | Binary Values |
|-----------|--------------|---------------|
| A         | 065          | 01000001      |
| I         | 105          | 01100100      |
| D         | 100          | 01100100      |

Programmers attempt to dissimulate much information in a picture, and then they require sufficient budgets of LSBs to secrete an information. These bits are situated in the picture pixels. Each pixel has three ingredients (R, G, and B). R, G, and B that include the Red, Green, and Blue ingredients of the pixel successively, supposing non-transparent picture, each of these ingredients be able have a importance between 0 and 255[7]. Currently the values of number of characters (LSBs) will be (pixels width x pixels height). Also, suppose that the picture was (400) pixels as height by (300) pixels as width, then LSBs will be equal (360000). And as each character can be typified by 8 bits, LSBs will be equal (45000). Then that image can secrete (45000) characters.

The LSB of each 8bit byte has been utilized to secrete a text message. It utilizes the first pixel (at spot 0) to secrete the length of message (number of character). And then, assume one can secrete a message in three pixels of a picture. Assume the original three pixels are:

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

A steganography software could secrete the character of message (J) which has a repose (74) into ASCII character position and have a binary representing "01001010", by alteration the channel bits of pixels.

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

In this situation, only four bits required to be varied to include the character swimmingly. The resultant revulsions that are caused to the LSB are few to be characterized by the human eye, therefore the message is actively secreted. Figure (4) exhibits a brief of image steganography algorithm [5].

Figure 4. A brief of image steganography algorithm.

1.2. Spatial Unsynchronization

Domain disconnection is a manner which bar from calibration assault. Domain disconnection (randomization) is a mechanism which is utilized for hiding the modulation domain from the intrusive.
The disconnection of the modulation field from the main field is used to bar camouflage data foretelling from the stego picture. In other signification, if the modulation field is preserved hidden from the intrusive then it is impossible to start calibration assault by foretelling the cover image site [1].

The spatial unsynchronization process is utilized to conceal the modulation field from the intrusive by randomizing the modulation domain. The locative unsynchronization indicates the modulation grid is not synchronized with the (JPEG) compression network of the stego picture. Due to this locative transition (unsynchronization), a noise (unsynchronization noise) is appurtenance to the stego picture. This noise hides the steganographic modulation in such a manner that the discovery of steganographic modulation turn into complicated for the intrusive. Thus locative transition process reacts standardization based assaults [8].

1.3. Fiber Tapping
Fiber tapping utilises a network tap manner that procures light signal from an optical fiber without shattering the communication. Tapping of cable of optical fiber enables diverting some of the light signal being dispatched in the core of the fiber into a sensor or another fiber. Bending is the expeditest and least discoverable method for hacking into a cable of fiber optic. Once the hacker gains access to the fiber optic cable and then executes the following steps as it shown in figure(5) and figure(6) [9].
1- Hacker installs a micro bend clamping equipment on it for leaking a little amount of signal of light.
2- Light signal is gathered by an optical photo sensor.
3- Light signal crosses through an optical electrical converter.
4- Optical electrical converter transfers the light signal via Ethernet connection to a laptop that analyzes it by utilizing specific software.

A tap reacts on confirmed modes which causing in each the other modes being reacted. This effect causes to energy becomes repeated from conductive to non-conducting modes and the apportionment of
power in the sheath and core of fiber are alterative. This alteration in power of modes be able utilized in the field of receiver by gauging the power included in the modes and then delimit if there is tapping or not. Fiber be able supervised by the optical average power standard being discovered [10].

The figure (7) shows the fiber optic cable diagram and the instantaneous power in the cable at any point along link's length, scaled properly to the cable drawing previous it. Also, this figure appears decrement in signals power, attenuation loss enlarges as the optical fiber length increases [9]. After all this argument, tapping comprises seizing portion of the optical signal. Therefore, OTDRs be able utilized to discover if there is tapping by monitoring the sites within the fiber path. The ratiocination shows that when the losses will become larger than specific threshold magnitude, then steganography mechanisms will be applied to the information for safety it [11].

2. Experimental Work
The experiment comprises transmitting information. Therefore, both encrypted text and file that secreted in cover picture carry over on optical system from one computer to the other. Beforehand, data is insured through cryptography and steganography at dispatcher's lateral computer with the visual basic software. Then information goes through optical media converter that ensample here optical fiber. Then information is taken and desired at receiver's lateral computer with the visual basic software.

Previously named hardware is connected as offered in figure (8). The PCI Fiber Optic Adapter acts in a 32-bit Bus Master Mode, giving (100Mbps) of speed with small stress on the host's CPU. The TE100-PCIFXplus bolsters both half and full duplex modes, invention an augmentation speed up to 200Mbps. With its SC-genre fiber liaison licensing up to (2Km) afar from the switch.

2.1. System Algorithm
This part discusses the suggested algorithm of steganography and acquirement of secret message. Algorithm uses the concept of encryption, spatial unsynchronization, randomization and hashing to execute full algorithm.

Step 1: Unsynchronize the cover picture (P) is by the picture cropping scheme, by eliminating (R) topmost rows and (C) left most columns. Get cropped picture (Pc) and residual part of picture (Pcr) as resultant, as shown in figure (9).

![Figure 9. Cropping Of (R) Topmost Rows and (C) Leftmost Columns.](image)

Step 2: Employ Hash function to transact aimless cropping on cropped picture (Pc). Obtain hashed cropped picture (Pch) and residual part of picture (Pchr) as resultant, as shown in figure (10).

![Figure 10. Aimless Cropping of Cover Image.](image)

Step 3: Secretion the text within the image

Program loops through the pixels of the picture. In each reiteration, obtain the RGB importance. Program makes the LSB equals to (0) for each of R, G, and B. These bits will be utilized in obscuring letters.

Program gets the present letter and mutates it to integer. Then secrete its 8 bits in R1, G1, B1, R2, G2, B2, R3, G3, where numerates mention to the ones of the pixels. In each LSB of these ingredients (from R1 to G3), secrete the bits of the letter successively.

Program processes the (8) bits of the letter, follows to the sequent letter, and iterates the process until the whole text is executed.

The text can be secreted in a little partition of the picture following to the length of that text. Therefore, there must be thing to refer that here software arrived the finish of the text. The indicant is simply (8) successively zeros. This will be required when deriving the text from the picture.

Step 4: encryption of the hidden data (Th). Obtain code text (Tc) as resultant.

Step 5: later the hashed cropped picture (Pch) is utilized for modulation code text (Tc) utilizing steganographic. Obtain stego picture (Ps1) as resultant.

Step 6: Stitch the stego picture (Ps1) with (Pchr) to obtain the modulated picture (Ps2).
Step 7: Stitch the picture ($P_s$) with ($P_c$) to obtain another modulated picture $P_m$.

After all to obtain the dissimulate message back, algorithm suggest following steps by considering ($P_m$) is the stego picture.

Step 1: take the value of $C$ & $R$ (number of cropped column and rows) from stego picture.

Step 2: unsynchronized the stego picture ($P_m$) is by the picture cropping scheme. Therefore, by eliminating ($C$) left most columns and ($R$) topmost rows. Obtain cropped picture ($P_c$) and residual part of picture ($P_{scr}$) as resultant.

Step 3: Execute Hash function to achieve aimless cropping on cropped picture ($P_c$). Obtain hashed cropped picture ($P_{sch}$) and residual part of picture ($P_{schr}$) as resultant.

Step 4: Then the hashed cropped picture ($P_{sch}$) is utilized for bit taking performance. Obtain code text of hidden data ($T_c$) as resultant.

Step 5: Deposing the text from the picture

It's more uncomplicated than secretion. Just pass through the pixels of the picture until program discovers (8) successive zeros. As soon as program is passing, collect the LSB from each pixel ingredient (R, G, B) and add it into an empty magnitude. When the 8 bits of this magnitude are done, mutate it back to letter, and then attach that letter to the result text.

Step 6: encore code text ($T_c$) to get the hidden data ($T_h$) as resultant.

3. Results and Discussion

Visual basic is a high fulfillment language for technical computing. In this paper, visual basic is executed for processing cryptography and steganography techniques. The technique of SUSA (Spatially Unsynchronized Steganographic Algorithm), secures that even when it's known that the picture is an information carrier, it is unimaginable to get back and organize the original bit sequence. SUSA uses matrix ($m \times n$) to secure files and encrypted text in the carrier picture in particular stego segments which are returned back to the picture. This system introduces a method that enciphers secret message and then embedding it in cover image. This paper also study the active embedding technology that can be employed for hiding the encrypted information in cover image to secrete it from hackers and sent message to the receiver in a safe manner. Figure(11) shows system program frame.

![Figure 11. System Program Form.](image)

Figure (12) shows frame of aboriginal message and encrypted text.
Figure 12. Original Text Message and encrypted text.

Figure (13) shows complex encrypted text.

Figure 13. Complex Encrypted Text.

Figure (14) shows aboriginal picture.

Figure 14. Aboriginal Picture

Figure (15) shows frame of steganography program that contains encrypted text and file (word file).
Figure 15. Steganography Program

Figure (16) shows stego picture.

Figure 16. Stego Picture.

Guarantee versus tapping can be done through observation of cable and signals. Therefore, observation signals can be expedite around fiber such that any try to bend the fiber will elevate the alarm. Optical fiber cable can also be observed with optical time domain reflectometer if attack of tapping is discovered within the fiber track. Pilot tone manner can also be utilized to discover disruptions of the sending. Each manner has weaknesses and strengths with respect to the tapping methods, and none can equip full guarantee. It is very complicated to supervise the complete fiber optics infrastructure. Therefore, cryptography and steganography can be the perfect reply to prevent tapping.

4. Conclusions

This paper introduces a fascinating and active method of hiding information comparative by other methods that has been utilized by programmers. Proper cryptography and steganography is safest technique, if users of optical communication networks want to keep unlegitimate eyes away from important data. This paper has affirmed the principle of securing information through cryptography and steganography both in terms of programs simulation and practical experiment.
References

[1] Alam S. and Depole D., “Analysis of Security Threats in Wireless Sensor Network” Int. J. Wir. Mob.Nets., Vol.6, No. 2, (2015), pp. 35-46.

[2] Dhamija A. and Dhaka V.,” A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration” Gr. Comp. Int. Things., 2015 Int. Con. IEEE, (2015 ), pp. 346-351.

[3] Krishnan S. and Abdullah M.S. “Enhanced Security Audio Steganography by Using Higher Least Significant Bit” J. Adv. Res. Com. App., Vol. 2, No.1, (2016), pp. 39-54.

[4] Sanjay K., Patil M., and Chitode J.S. “ Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image Steganography Employing FPGA” Int. J. Image, Gra. signal Processing., Vol. 6, No.1, (2016), pp. 48-56.

[5] Elshazly E.A., Fikry R.M., and Zahran O. “FPGA Implementation of Robust Image Steganography Technique based on Least Significant Bit (LSB) in Spatial Domain” Int. J. Computer App., Vol. 145, No.12, (2016), pp. 43-52.

[6] Osunade O. and Ganiyu I.A. “Enhancing the Least Significant Bit (LSB) Algorithm for Steganography” Int. J. Computer App., Vol. 149, No.3, (2016), pp. 1-8.

[7] Hiary H., Eddin K., Mohammed M.S., and Dhamari A. “A Hybrid Steganography System based on LSB Matching and Replacement” Int. J. Adv. Computer Sci. App., Vol. 7, No.9, (2016), pp. 374-380.

[8] Sinha S. and Gupta P. “Image Steganography Using Desynchronization” Int. J. Computer Sci. Mob.Computing., Vol. 5, No.2, (2016), pp. 55-61.

[9] ZafarIqbal M., Fathallah H. and Belhadj N. “Optical fiber tapping: Methods and precautions” High Capacity Opt. Nets.Enabling Tec., 2011.IEEE., (2011), pp.164-168.

[10] Gabriel Etim U. and Aniefiok Out A. “The Vulnerability of Fiber-Optics Communication Systems: The Role of Optical Tapping” J. Info. Eng. App., Vol. 4, No.4, (2014), pp.145-153.

[11] Rawat B. and Sone M. “Securing Data in Fiber Optics” Int. J. Res. Applied. Sci. Eng. Tech., Vol. 2, No.6, (2014), pp. 162-166.