

Secure Optical Link System

Shubham Pandey¹, Ruchi Varshney², Shivani Gupta¹, Sangeeta Singh¹, Neha Chaudhary¹

UG Scholars, Dept. of ECE, MIT Moradabad, Ram Ganga Vihar, Phase II, Moradabad, India¹

Assistant Professor, Dept. of ECE, MIT Moradabad, Ram Ganga Vihar, Phase II, Moradabad, India²

Abstract: With the explosion of information traffic due to the Internet, electronic commerce, computer networks, multimedia, voice, data, and video, the need for a transmission medium with the bandwidth capabilities for handling such vast amounts of information is paramount. Fiber optics, with its comparatively infinite bandwidth, has proven to be the solution. The security inherent in optical fiber systems is a major benefit. The increasing rate of crime, attacks by thieves, intruders and vandals, despite all forms of security gadgets and locks, still need the attention. To make optical link more secure many devices can be used for transmission and reception purpose. These devices may be DNA sensor lock, card sensor lock, electronic eye lock, thumbprint sensor lock and electronic combination lock. In this research paper we are focusing on a secure communication where biometric system can be used as a good and effective security option. An important and very reliable human identification method is fingerprint identification. As fingerprint of every person is unique thus it can be used in various security options. Fingerprint recognition at the transmitter side allows only valid person to transmit the signal. At the receiver side code lock security can be economic and good option to allow only valid user to receive the information which has been sent through secure optical link. During communication over the optical link, automation can also be achieved at the receiver end from the transmitter end. With the help of automation, energy consumption at the receiver end can be reduced upto a great extent from the transmitter end.

Keywords: Automation, Biometric security, Code-lock security, Optical fiber link.

I. INTRODUCTION

Data transmission through unguided transmission media leads to less security availed in the transmission therefore data is lost easily during transmission. Data transmission through guided media leads to a point to point communication which is comparatively more secure than unguided media transmission. There are multiple examples of guided media transmission such as coaxial cable, twisted pair and optical fiber transmission. These media have their own data transmission capacity. Optical fiber cable has the largest data transmission capacity among them. The usual rate for optical fiber cable systems is 2.4 Gbps or even 10 Gbps. While giving high data transmission rate optical fiber is also provides secure data transmission.

There is a consequent increase in the rate and sophistication of crime. As a result, it is necessary to ensure security of oneself and one's valuable belongings. This creates demand of a new and modern lock that must be unique. This type of feature is available in the biometric locks i.e. the lock which can only be locked and unlocked by the human body features. Fingerprint of every person on the earth is unique and can provide good reliability. Also the implementation of the fingerprint recognition system is easy and economic than the other ones^[14]. Biometric security can be used at transmitter end so no unauthorized person is able to send any kind of wrong information to the receiver end. Receiver end requires a security system too. So a code-lock security system protects the receiver end. Only a person who has valid

password can be able to unlock the received data. With the increase in consumption of energy, there is a great need to conserve energy in every way possible. The inability to access and control the appliances from remote locations is one of the major reasons for energy loss. So automation is also introduced in the project to control energy consumption^[12].

II. LITERATURE SURVEY

Nick Massa [9]:

This paper states that optical fiber must be protected from the environment. Cabling provides the fiber protection from the elements, added tensile strength for pulling, rigidity for bending, and durability. In general, fiber optic cable can be categorized into two types:

1) Indoor Cables:

- Simplex cable-contains a single fiber for one-way communication
- Duplex cable-contains two fibers for two-way communication
- Multi fiber cable-contains more than two fibers. Fibers are usually in pairs for duplex operation.
- Breakout cable-typically has several individual simplex cables inside an outer jacket. The outer jacket includes a zip cord to allow easy access.
- Heavy, light, and plenum-duty and riser cable:
 - Heavy-duty cables have thicker jackets than light-duty cable, for rougher handling.



- Plenum cables are jacketed with low-smoke and fire-retardant materials.
 - Riser cables run vertically between floors and must be engineered to prevent fires from spreading between floors.
- 2) Outdoor Cables:** Outdoor cables must withstand harsher environmental conditions than indoor cables. Outdoor cables are used in applications such as:
- Overhead-cables strung from telephone lines
 - Direct burial-cables placed directly in trenches
 - Indirect burial-cables placed in conduits
 - Submarine-underwater cables, including transoceanic applications.

Fiber Optic System Design Considerations:

1) Power Budget: The power arriving at the detector must be sufficient to allow clean detection with few errors. The power at the detector must be above the threshold level or receiver sensitivity.

2) Bandwidth and Rise Time Budgets: The transmission data rate of a digital fiber optic communication system is limited by the rise time of the various components, such as amplifiers and LEDs, and the dispersion of the fiber. The cumulative effect of all the components should not limit the bandwidth of the system.

3) Connectors: Many types of connectors are available for fiber optics, depending on the application. The most popular are:

- SC-snap-in single-fiber connector
- ST and FC-twist-on single-fiber connector
- FDDI-fiber distributed data interface connector

4) Fiber Optic Couplers: A fiber optic coupler is a device used to connect a single (or multiple) fiber to many other separate fibers. There are two general categories of couplers:

- a) Star couplers
- b) T-couplers

5) Wavelength-Division Multiplexers: The couplers used for wavelength-division multiplexing (WDM) are designed specifically to make the coupling between ports a function of wavelength. The purpose of these couplers is to separate (or combine) signals transmitted at different wavelengths. Essentially, the transmitting coupler is a mixer and the receiving coupler is a wavelength filter.

Annie P. Oommen, Rahul A P, Pranav V, Ponni S and Renjith Nadesan [1]: This paper explained how to create a micro-controller based Digital Code Lock that serves the purpose of security. The microcontroller based Digital Code Lock is an access control system that allows only authorized persons to access a restricted area. The system comprises of a push button keypad connected to the 8 bit microcontroller. The system will allow you to preset a password. The lock will open if and only if the entered password matches the preset one. If the entered password is wrong a buzzer will be activated. In our project digital code lock comprises of 8 bit microcontroller AT89s52.

Adamu Murtala Zungeru [2]: In his paper, he explained that the use of electronic combination locks in modern day

technology cannot be overemphasized. They prevent losses to theft, carelessness etc. Also being that they are electronically powered, they provide a better and safer security system than all other locks. The block diagram of the electronic lock contains power supply unit, the input, control and the output units as shown in fig. 1.

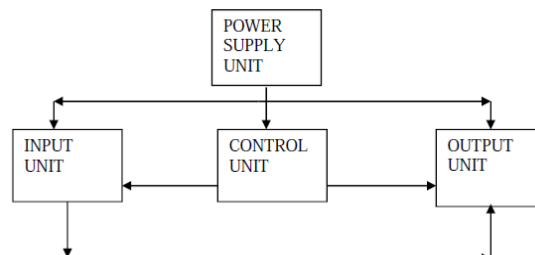


Fig. 1. Block diagram of Electronic Switch^[2]

Vaclav Matyas and Zdenek Riha [10]: He proposed the classification of biometric on different parameter in his paper. Biometric systems falling into the level four should be able to resist even professional and well-funded attacks.

TABLE I CLASSIFICATION OF BIOMETRIC ON DIFFERENT PARAMETER^[10]

Level	Live-ness	Temperature resistance	Secure comm.	Traditional auth method
1	No	No	No	Sufficient/ Anytime
2	No	No	Yes	Sufficient/ Malfunction
3	Yes	Moderate	Yes	Not sufficient
4	Multiple	Advanced	Yes	Not sufficient/ Required

Artur Balanuta Ricardo Lopes Pereira and Carlos Santos Silva [6]: In his paper he proposed a novel system to address the energy consumption problem and inadequate habits of people in office buildings. It's a highly flexible distributed office management system that can scale from an individual node in an office to the whole building. The goal is to reduce global building energy consumption without significantly affecting the user's comfort level. An approach is used where the building services are adjusted to its occupancy level and user's needs based on their location. Users are driven to better energy usage habits through access to information and feedback.

Ravi Subban and Dattatreya P. Mankame [8]: In his paper he focused on knowledge on the diverse area of FP biometric systems envisage the importance of FP biometric system to provide strong authentication. The FR is having edge over other biometric traits. Our project uses fingerprint security.

TABLE II PERFORMANCE OF DIFFERENT BIOMETRIC TECHNOLOGIES BASED ON EER, FAR AND FRR ^[8]

Biometric	EER	FAR	FRR
Face	NA	1%	10%
Fingerprint	2%	2%	2%
Hand geometry	1%	2%	2%
Iris	0.01%	0.99%	0.94%
Key Strokes	1.8%	7%	0.1%
Voice	6%	2%	10%

Anil K. Jain, Arun Ross and Salil Prabhakar [3]: In his paper he explained the practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system. In this paper, he provided a brief overview of the field of biometrics and summarized some of its advantages, disadvantages, strengths, limitations, and related privacy concerns.

Ritesh A. Jadhav and Dattatraya S. Shitole [5]: This paper explained the implementation of fiber optics in electronic communication network with development in optical fiber communication. Its high bandwidth capabilities and low attenuation characteristics make it ideal for gigabit transmission. Using fiber optic cable, optical communication have enabled communications links to be created over much greater distances and with much lower levels of losing the transmission medium and possibly most important to fall, fiber optical communications has enabled much higher data rates to be accommodated.

Satish Palaniappan, Naveen Hariharan, Naren T Kesh, Vidhyalakshimi S and Angel Deborah S [7]: He explained in his paper that remotely accessible environment is an environment in which each appliance can be remotely accessed and controlled. Such remotely accessible systems are already available in the market, but have a number of drawbacks as well. So we are providing automation in our project using optical fiber, which is comparatively much better than other.

Neha Chaudhary Sangeeta Singh, Shubham Pandey and Shivani Gupta [11]: This paper showed the study of optical fiber and different types of security which can be used while transmitting or receiving data. The single mode fiber optic cable provides much better performance with lower attenuation. She explained different types of biometric security e.g. Voice Recognition, Signature Recognition, Face Recognition, Palm scan, Iris-scan, Retina-scan, Hand geometry, Signature-scan, Fingerprint Recognition etc. This paper introduced a proposal in which one can use advance technologies like biometric, code lock and optical link for the safe and secure

transmission of information. She explained in her paper that Optical Fiber Link is very secure medium for voice and data transfer. The finger print module helps to transmit the data from an authorized person only whereas code lock at the receiver end is used for receiving information by an authorized person. At receiver end the lock will open only if entered password matches the preset one otherwise not. The brief study in this paper has shown how code lock security works. The advantage of this code lock is that the password will be in encrypted form so that no other person will be able to understand the password.

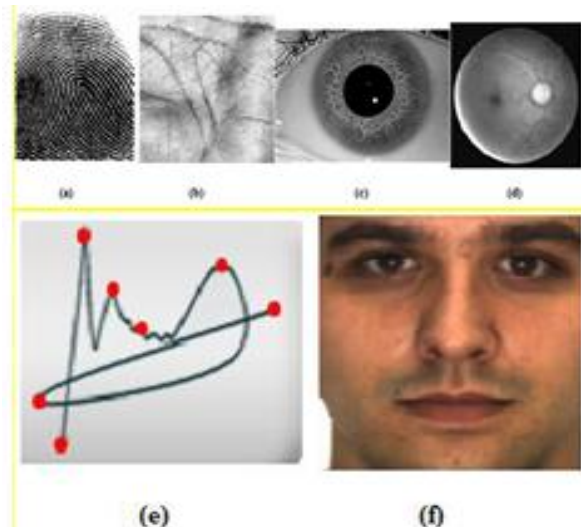


Fig. 2. Biometrics traits (a) Fingerprint (b) Palm (c) Iris (d) Retina (e) Signature (f) Face ^[11]

Shubham Pandey, Shivani Gupta, Neha Chaudhary and Sangeeta Singh [12]: He focused on advancement of neha chaudhary et al proposal. Further study is carried out by him in this paper. This paper showed the study of different types of biometric security and how biometric security works in real time world. He explained how biometric is depending upon the application context, a biometric system may operate either in verification mode or identification mode. He also provided the study of optical fiber link and code lock security. He discussed the evolution and advantages of the optical fiber. He further introduced an automation process in previous proposal so that energy consumption can be reduced. Study of automation is also shown in this paper. He also introduced the proposed model of the project in his paper and explained the modes of project. The project can be classified into following modes-

A) Biometric:

- 1) Data base mode
- 2) Valid casting mode
- 3) Checking mode

B) Optical Link Mode: In this mode optical fiber is used for communication purpose.

- 1) Voice communication
- 2) Data communication
- 3) Fail mode of optical link

C) **Code Lock:** Code lock security is used at receiver end, when any person enters code, system will check condition and operate the optical link.

D) **Automation:** As the name suggests for getting something done automatically. This project proposal is to achieve automation at the receiver end and get it done from the transmitter end.

III. PROBLEM IDENTIFICATION

The problem for which this project idea is demonstrated is consequent increase in the rate and sophistication of crime. As the result of increment in crime it is highly demanding to make communication more secure. So to provide security biometric, code lock and RF-ID etc. technologies can be used.

While demonstrating this project we have faced some problems. Some problems occurred designing the circuit and others occurred implementing the project. The problem faced in designing are listed below:

- 1) Components availability.
- 2) Deciding value of components.
- 3) Circuit designing.

The problems faced during implementing the project are listed below:

- 1) How to give the effort of soldering properly.
- 2) Programming of sensor.
- 3) Signal sending.
- 4) LCD interfacing.
- 5) Buzzer interfacing at receiver end.
- 6) Finger print module interfacing at transmitter end.

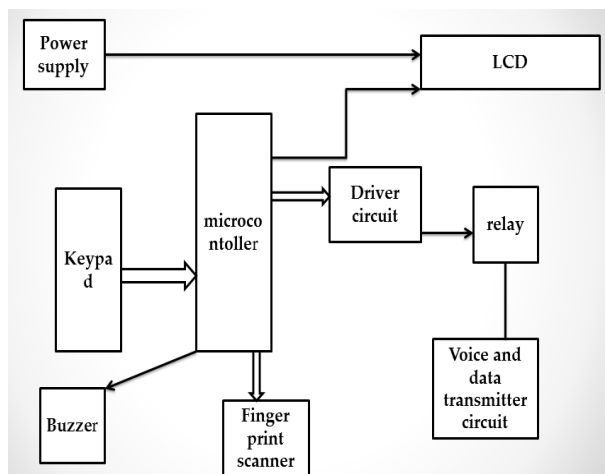


Fig. 3. Block diagram of proposed project [12]

Sangeeta Singh, Neha Chaudhary, Shubham Pandey and Shivani Gupta [13]: She further carried out research on the project proposed by Shubham Pandey et al. She explained more modifications in the proposed block diagram and further introduced the circuit diagram of the transmitter and its working in her paper. She explained that the heart of the circuit is microcontroller at89s52. Other components used are voltage regulator 7805, LCD display 16x2, matrix keypad, relay, buzzer, and finger print scanner. First of all, step down transformer and rectifier together converts 220 AC voltage into 12V DC supply and capacitor is used to reduce the harmonics those are introduced during rectification and regulator 7805 IC provides fixed five volts. Data can be sent either using keypad or using mic.

IV. DESIGN AND IMPLEMENTATION

Optical fiber cable has the largest data transmission capacity. The usual rate for optical fiber cable systems is 2.4 Gbps or even 10 Gbps. While giving high data transmission rate optical fiber is also provides secure data transmission. An important and very reliable human identification method is fingerprint identification. As fingerprint of every person is unique thus it can be used in various security options. Fingerprint recognition at the transmitter side allows only valid person to transmit the signal. At the receiver side code lock security can be economic and good option. Automation can also be performed through optical link in this project. The block diagram of this project is shown in the figure 5. After verifying the biometric ID proof that is fingerprint of an authorized person, the optical transmitter sends the analog or digital signal through optical fiber cable, which is then received by the optical receiver. In case of invalid person at the transmitter end, system will beep and doesn't provide access to an unauthorized user. This optical link can also be used for controlling different devices at receiver end. After reception of the signal at the receiver end, the user would be able to access the data and the transmission would be successfully done with higher security.

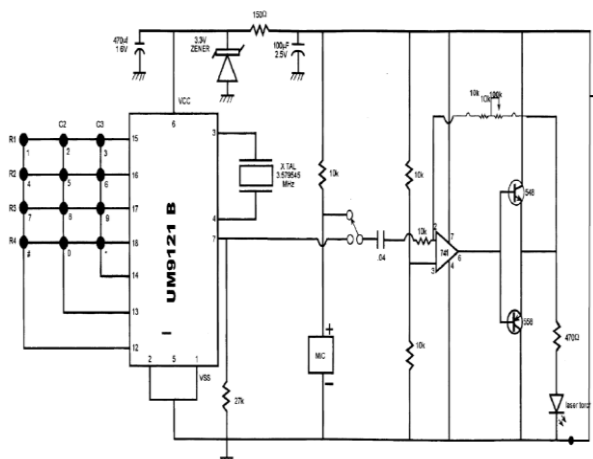


Fig. 4. Circuit Diagram of Transmitter [13]

A regulated power supply of 5 volts is needed in this project. When user wants to send the data and voice with the help of optical fiber, system will demand for fingerprint scanning. Then system will check the fingerprint condition and operate the relay in case of valid fingerprint and allow communication of voice and data. Microcontroller then allows driver circuit to activate the relay; this will create an optical fiber link.

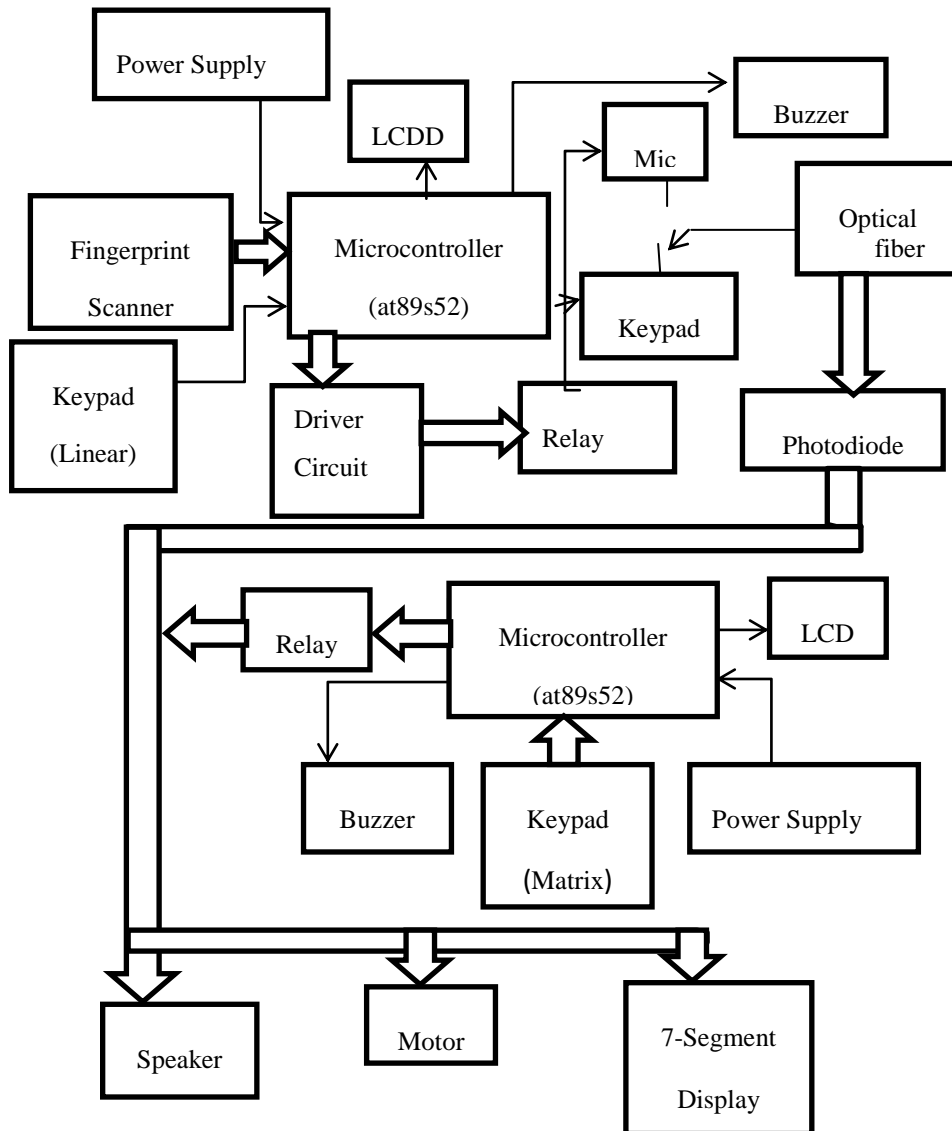


Fig. 5. Block Diagram of The Project

In case of invalid user the buzzer gives indication and it gets displayed on LCD display that the user is unauthorized and the link will not be created. Photodiode at the receiver receives the information. Only when the valid password is entered through keypad (matrix), microcontroller will allow relay to operate. Then received information can be gained through speaker/ motor or 7-segment display. If user enters wrong password then buzzer will beep and "INVALID USER" gets displayed on LCD display.

Working:

First of all, step-down transformer and rectifier are used to convert 220 AC voltage into 12 volts DC supply. Capacitor is used to remove the harmonics those are introduced during rectification and regulator 7805 IC is used to provide fixed 5 volts.

Biometric Module: We enter the database in the biometric module with the help of keypad (linear) and

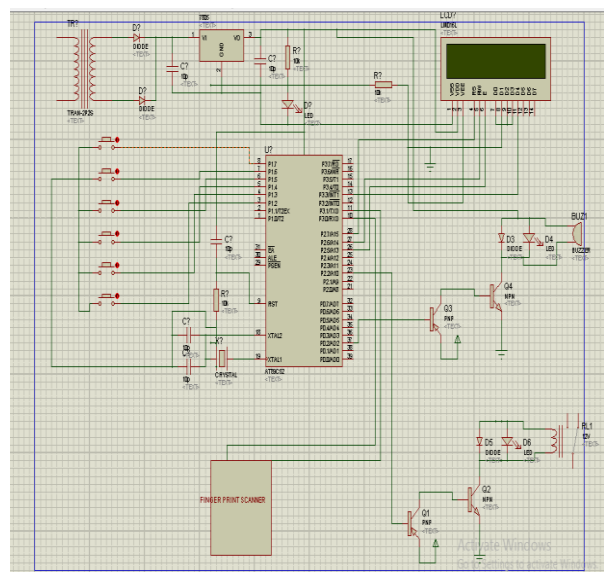


Fig. 6. Simulation of Biometric Module

fingerprint scanner. All conditions are displayed on LCD display. Through fingerprint scanner the condition of valid user will be checked and be displayed on LCD display. In case of valid user microcontroller (at89s52) then allows driver circuit to activate the relay; this will create an optical fiber link. In case of invalid user the buzzer will give indication.

Optical Fiber Communication: The optical fiber communication involves two types of data transmission that are analog and digital data transmission. In our project we are using both types of data transmission. First one is analog signal i.e. voice signal using mic and other one is digital signal using numeric keypad. We use switch to change over data transmission type. An optical fiber data transmission basically involves three components: an optical transmitter, an optical fiber cable and an optical receiver.

Transmitter: For digital input we use DTMF signal generator (UM91514) for generating a signal in the form of PWM (pulse width modulation.). All the nine switches are connected to the input of this IC as a matrix network. All the switches are divided in four rows and three columns. Pin no 6 of this IC is connected to the positive supply. This IC is very sensitive to voltage and requires only 3.3 voltage. Zener diode regulated supply is used for this requirement. 150Ω resistance is used to limit the current. One crystal is connected to the 3rd&4th pin of this IC to provide a carrier frequency to the IC. Output is available on the 7th pin of this IC which is directly connected to the 2nd pin of OP-AMP IC. Switch is provided to change the input to either digital or analog. Voice data is fed through mic as an analog input which converts this mechanical signal into electrical signal and coupled at the 2nd pin of OP-AMP IC (741). Pin no. 3 acts as a comparator. 7th pin of 741 IC is connected to the power supply and 4th pin is grounded. 741 IC is used as amplitude amplifier.

The amplification factor depends upon the negative feedback which is connected between 2nd and 6th pin of this IC. The amplified output is taken from 6th pin of OP-AMP IC. For further power amplification transistor circuit is used. Here we use two transistors one is NPN and second is PNP. Collector of the NPN is connected to the positive supply and collector of the PNP is connected to the negative supply. Output is available from the emitter of the both transistor.

The output of this transistor circuit is connected to the semiconductor laser diode. Working voltage of this diode is approx. 3.6 volt. This diode is very sensitive and on high voltage it is immediately burnt out. Here Ga-As laser is used. Output from the amplifier is further converted into regulated 3.6 voltage with the help of one 3.6 volt zener diode. Zener diode is used with laser light to protect them from high voltage. Data is now super imposed on the laser light and we focus this laser light towards the receiver.

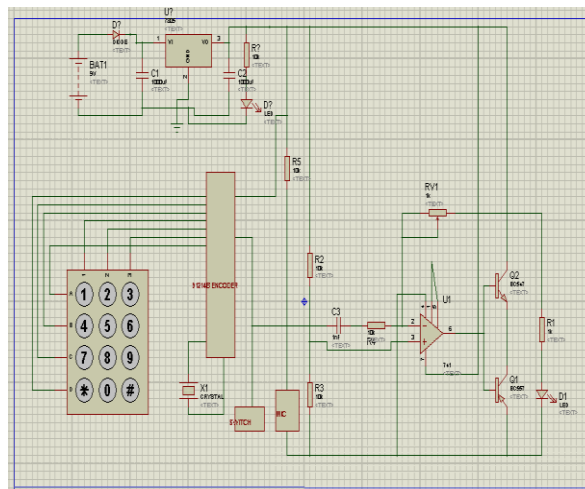


Fig. 7. Simulation of Transmitter

Receiver: The laser light is received on the photodiode at the receiver section. Photodiode converts this light into electrical signal. This small voltage is amplified by OP-AMP IC. The output of 741 IC is further amplified by the transistor pair, this amplification is power amplification. Then voice output is available at the speaker or in case of digital signal, it is further fed to the DTMF decoder (CM8870C). DTMF decoder converts this signal into a BCD signal. This is a 18 pin IC. Pin no. 10 and 18 is connected to the positive supply. One crystal is connected to the pin no. 7 and 8 to demodulate the frequency. Signal from the operational amplifier is applied to the pin no 2 and 3 of this IC.

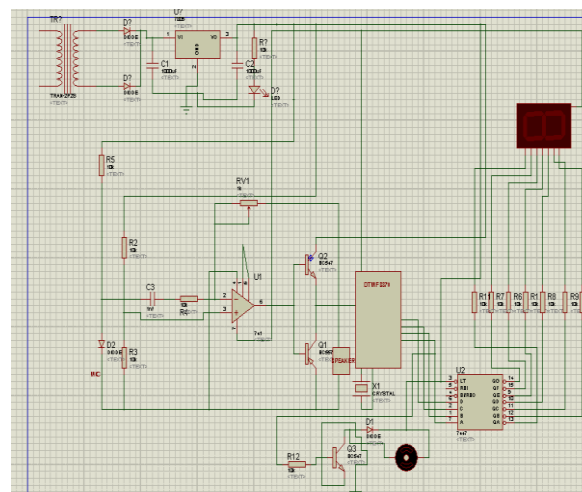


Fig. 8. Simulation of Receiver

The demodulated frequency is available on the pin no 11, 12, 13, 14 in the form of BCD signal. This BCD signal is used to control many other appliances, so with the help of this BCD signal automation is achieved at the receiver end. This BCD signal is also used to display the digital data on 7-segment display. IC 7447 is used as a seven segment decoder circuit. IC 7447 receives the BCD signal from the 8870 and convert this signal in the numeric display.

Code-Lock: At the receiving end user needs to verify his identity to access the received data. User has to enter valid password to obtain information from the system. In case of invalid password the buzzer will beep and “INVALID USER” gets displayed on the LCD display. Or in case of valid user microcontroller will allow relay to operate. Then according to the signal either it is displayed on 7-segment display or can be heard by speaker. Automation can also be shown by applying any appliance at the receiver end.

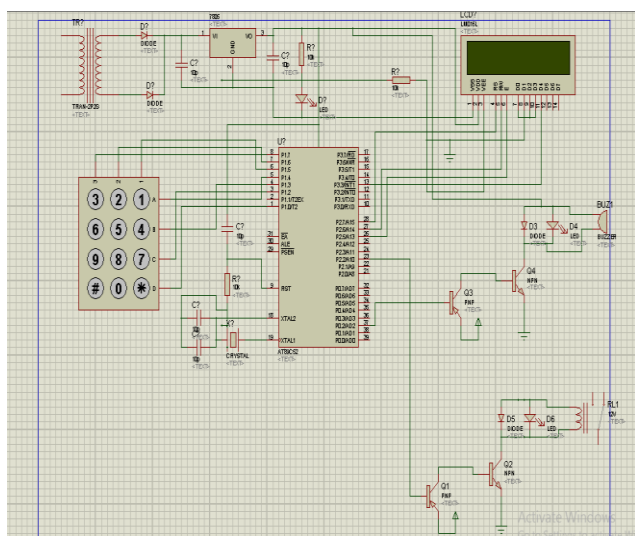


Fig. 9. Simulation of Code-Lock

V. RESULTS AND DISCUSSION

The result of this project came as expected. Result of the project is that by using this advance and intelligent optical link system we can transmit and receive the data through an authorized person only, no other person can send and receive the data through this link and hence this device can do wonders in the field of communication. After working upon this we achieved more advancement in security system and with the help of this project optical link automation can also be performed that means user can control different appliances from one place (from transmitter end). Fingerprint module provides higher security for the data transmission. Code lock is another way to secure the data. Optical fiber link provides high speed in transmission. It is clear that every technology has its advantages as well as limitations. So it is better to merge the technologies to reach a desired goal as a group of technologies when used together can overcome each other's limitations and hence it results in a better project. This project may find a great use in field of communication and automation as it is fulfilling many tasks that include secure digital and analog data transmission and automation.

This project has a drawback of not having a storing element to record the data for receiving it after some time at the receiver side.

VI. CONCLUSION

Based on all the systems surveyed and their advantages and drawbacks studied, this paper presents an integrated technology that can enable a user to communicate in a secure way. Through optical link user can send data at very high rate and in a secure manner. Optical link provides analog and data transmission both. The biometric technology enhances the security so we conclude that it would be used at transmitter side so that only a valid person, whose data has been stored in data base, can transmit the data. Fingerprint identification is reliable security device. Code-lock is also a good and economic option for security purpose. Therefore it is used here at the receiver side. Hence this device can do wonders in the field of communication.

Automation is also provided from the transmitter end. Hence many tasks can be performed easily from the transmitter end with less physical effort and therefore energy consumption can be reduced upto a great level. This technique will be very useful for colleges, banks, and other important places.

VII. FUTURE SCOPE

Whether it's a technology, human, device or machine, there is always a place for improvement to make it better; same is in the case of this proposed work. As we are merging different technologies, more advancement can be achieved in the future. First of all we can add a storing element in this technology so that at receiver data can be received by the user even after some time too. Multi – Terabit Optical Networks Dense Wave Division Multiplexing (DWDM) can be used to provide higher bandwidth for data transmission. More understanding of the interactions between the electromagnetic light wave and the transmission medium is necessary to proceed towards an infrastructure with the most favourable conditions for a light pulse to propagate. Improvement in laser technology can also be introduced here. The use of ultra-fast photonic sections is expected to further improve the capacity and speed of telecommunication networks.

REFERENCES

- [1] Annie P. Ommen, Rahul A P, Pranav V, Ponni S, Renjith Nadeshan, “Design and Implementation of a Digital Code Lock” Published in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2278 – 8875, Volume- 3, Issue 2, February 2014.
- [2] Adamu Murtala Zungeru , “An Electronic Digital Combination Lock: A Precise and Reliable Security System”, School of Electrical and Electronic Engineering, University of Nottingham, Jalan Broga, 43500 Semenyih, Selangor Darul Ehsan, Malaysia.
- [3] Anil K. Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition”, Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.
- [4] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric Recognition: Security and Privacy Concerns”, IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, 2003.

- [5] Ritesh A. Jadhav, Dattatraya S. Shitole, "FIBER OPTICS COMMUNICATION AND APPLICATIONS" published in International Journal of Innovative Research in Engineering & Science, ISSN 2319-5665, issue 2, volume 4, April 2013.
- [6] Artur Balanuta, Ricardo Lopes Pereira and Carlos Santos Silva, "Personal Office Management and Automation System" published in 23 July 2015 in IEEE Distributed Computing in Sensor Systems (DCOSS), 2015 international conference on 10-12 June 2015.
- [7] Satish Palaniappan, Naveen Hariharan, Naren T Kesh, Vidhyalakshmi S, Angel Deborah S "Home Automation Systems - A Study", published in International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 116, April 2015.
- [8] Ravi subban and Dattatreya P. Mankame "A Study of Biometric Approach Using Fingerprint Recognition", Vol. 1, No. 2, May 2013.
- [9] Nick Massa, "Fiber Optic Telecommunication", fundamentals of photonics, pg. 293-347.
- [10] Vaclav Matyas and Zdenek Riha, "Biometric Authentication-Security And Usability".
- [11] Neha Chaudhary, Sangeeta Singh, Shubham Pandey and Shivani Gupta "A Review Paper on Optical Communication using Biometric and Code Lock", published in Imperial Journal of Interdisciplinary Research, ISSN: 2454-1362 Vol-2, Issue-11, 2016.
- [12] Shubham Pandey, Shivani Gupta, Neha Chaudhary and Sangeeta Singh "Study Of A Secure Communication System", published in Imperial Journal of Interdisciplinary Research, ISSN: 2454-1362 Vol-2, Issue-11, 2016.
- [13] Sangeeta Singh, Neha Chaudhary, Shubham Pandey and Shivani Gupta "Secure Communication And Automation Using Optical Link", published in Northern Asian International Research Journal Consortium, ISSN: 2454-7514 Vol-3, Issue-3, March 2017.
- [14] Amit Saxena, Sarthak Sharma, Shivam Gaur, Shubham Chauhan, Shantanu Varshney, "IGNITION BASED ON FINGERPRINT RECOGNITION", published in International Journal of Scientific Research and Management Studies (IJSRMS), ISSN: 23493771, Vol. 2, Issue 1, pg. 66-71.
- [15] Fair, I. J., Grover, W. D., Krzymien, W.A. and MacDonald, R.I., "Guided Scrambling: A new coding technique for high bit rate fiber optic transmission systems," IEEE Transactions on Communications, vol. 39, no. 2, p. 293, February 1991.
- [16] Understanding Optical Communications by Harry J. R. Dutton International.
- [17] Halliday, Resnick, and Kenneth S. Krane. Physics 4th Ed. Canada. 1992, pp. 905.
- [18] M. Noshada, A. Rostami, "FWM minimization in WDM optical communication systems using the asymmetrical dispersion managed fibers", International Journal for Light and Electron Optics, vol. 123, no. 9, pp. 758– 760, 2012.
- [19] X. Wang and K. Kitayama, "Analysis of beat noise in coherent and incoherent time-spreading OCDMA," IEEE/OSA Journal of Lightwave Technology, vol. 22, no. 10, pp. 2226-2235, 2004.
- [20] Mable P. Fok "Optical Layer Security in Fibre Optic Networks" published in IEEE Transactions on Information Forensics and Security Volume- 6, Issue 3, 2011.
- [21] Shunshan li, Min Wei, Haiying Tang, Tiange Zhuang and Michael H. Buonocore, "Image Enhancement Method for Fingerprint Recognition System.", Proceedings of the 2005 IEEE, Engineering in Medicine and Biology 27th Annual Conference, Shanghai, China, September 1-4, page no. 3386-3389, 2005.
- [22] Fiber-Optic Telecommunication and the Economic Benefits of a Better ICT Infrastructure in the Context of Bangladesh by Shabbir Bashar.
- [23] A. K. Jain and A. Ross, "Learning User-specific Parameters in a Multibiometric System", Proc. International Conference on Image Processing (ICIP), Rochester, New York, September 22-25, 2002.
- Ruchi Varshney** is having 14 years of experience in the field of Electronics & Communication. She has published number of papers in National and International Journals and Conferences. Area of interest includes wireless, MATLAB, communication, embedded.
- Shivani Gupta** is pursuing B.Tech in Electronics & Communication Engineering from Moradabad Institute of Technology, Moradabad. Area of interest includes wireless, MATLAB, communication.
- Sangeeta Singh** is pursuing B.Tech in Electronics & Communication Engineering from Moradabad Institute of Technology, Moradabad. Area of interest includes wireless, MATLAB, communication, embedded.
- Neha Chaudhary** is pursuing B.Tech in Electronics & Communication Engineering from Moradabad Institute of Technology, Moradabad. Area of interest includes wireless, MATLAB, communication, embedded.

BIOGRAPHIES

Shubham Pandey is pursuing B.Tech in Electronics & Communication Engineering from Moradabad Institute of Technology, Moradabad. Area of interest includes wireless, MATLAB, communication, embedded.