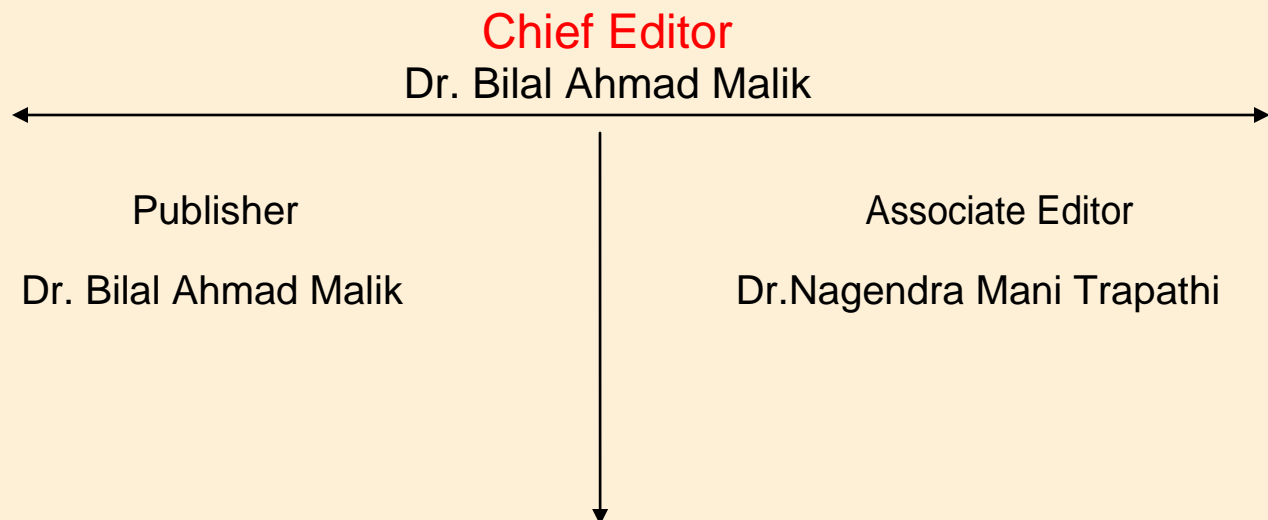


North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology



NAIRJC JOURNAL PUBLICATION

North Asian
International
Research Journal Consortium



Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

M.C.P. Singh Head Information Technology Dr C.V. Rama University	S.P. Singh Department of Botany B.H.U. Varanasi.	A. K. M. Abdul Hakim Dept. of Materials and Metallurgical Engineering, BUET, Dhaka
Abdullah Khan Department of Chemical Engineering & Technology University of the Punjab	Vinay Kumar Department of Physics Shri Mata Vaishno Devi University Jammu	Rajpal Choudhary Dept. Govt. Engg. College Bikaner Rajasthan
Zia ur Rehman Department of Pharmacy PCTE Institute of Pharmacy Ludhiana, Punjab	Rani Devi Department of Physics University of Jammu	Moinuddin Khan Dept. of Botany Singhaniya University Rajasthan.
Manish Mishra Dept. of Engg, United College Ald.UPTU Lucknow	Ishfaq Hussain Dept. of Computer Science IUST, Kashmir	Ravi Kumar Pandey Director, H.I.M.T, Allahabad
Tihar Pandit Dept. of Environmental Science, University of Kashmir.	Abd El-Aleem Saad Soliman Desoky Dept of Plant Protection, Faculty of Agriculture, Sohag University, Egypt	M.N. Singh Director School of Science UPRTOU Allahabad
Mushtaq Ahmad Dept.of Mathematics Central University of Kashmir	Nisar Hussain Dept. of Medicine A.I. Medical College (U.P) Kanpur University	M.Abdur Razzak Dept. of Electrical & Electronic Engg. I.U Bangladesh

Address: -North Asian International Research Journal Consortium (NAIRJC) 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815, Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

SECURE COMMUNICATION AND AUTOMATION USING OPTICAL LINK

SANGEETA SINGH¹, RUCHI VARSHNEY², NEHA CHAUDHARY¹, SHUBHAM PANDEY¹ & SHIVANI GUPTA¹

¹U.G. Scholars, Dept. of E&C Engg., MIT Moradabad
Ram Ganga Vihar, Phase II, Moradabad (244001), India
²Assistant Professor, Dept. of E&C Engg., MIT Moradabad
Ram Ganga Vihar, Phase II, Moradabad (244001), India

ABSTRACT

This paper deals with communication using optical fibre. The optical fibre is chosen as a medium in communication system because of its characteristics which include small size or dimension, low loss and low interference from outside. The rate of crime, intruders is increasing day by day and the security gadgets still need to be modified so that we can make the transmission of information more secure so in this technology the biometric module used is finger print scanner at the transmitter end and code lock at receiver end over other security modules. Code lock system allows the user to unlock the device with a password. By this technique data is transmitted in secure manner by first scanning the finger print and entering the link and then at receiver side first a user defined password is entered, then only information is received by the authorized person i.e. the one who knows the user defined password.

KEYWORDS: Fingerprint module, Keypad, Code Lock Module, LCD Screen, Microcontroller AT89s52

1. INTRODUCTION

In this technology Optical fiber is selected as medium for communication in a very secure way. The advantages of optical fiber communication with respect to copper wire systems are broad bandwidth, immunity to electromagnetic interference, low attenuation loss over long distances, electrical insulator, material cost and theft prevention and security of information passed down the cable. Security level increases the demand of such type of lock which is new and provides an additional security level. The finger print scanner helps to transmit the data through an authorized person only whereas code lock at the receiver end is also used for receiving of information through authorized person. At receiver end the lock will open only if entered password matches the preset

otherwise not. In this technology both analog and digital data can be sent through the link and hence automation is also done. Code lock at the receiver side helps in the transmission of data in a secure and effective manner without any leakage of the important information and can only be received by the authorized person by the code lock technique.

2. LITERATURE REVIEW

Ravi Subban et al explained in his paper the research work carried out in Finger print matching techniques, recognition methods and their performance analysis. The proposed system uses finger print module at the transmitter end for identification of persons through finger prints stored in the database. Finger print identification is popular biometric technique due to easiness in acquiring, availability of plenty sources (i.e. ten fingers) for collecting data and their established use. He explained that a biometric system contains mainly an image capturing module i.e. finger print module, a feature extraction module and a pattern matching module as shown in Fig. 1. An image capturing module acquires the raw biometric data of a person using a sensor. Utilizing suitable algorithm/s feature extraction module improves the quality of the captured image. Database module stores the biometric template information of enrolled Persons. Pattern matching module compares the extracted features with the stored templates, which in-turn generates match score [1].

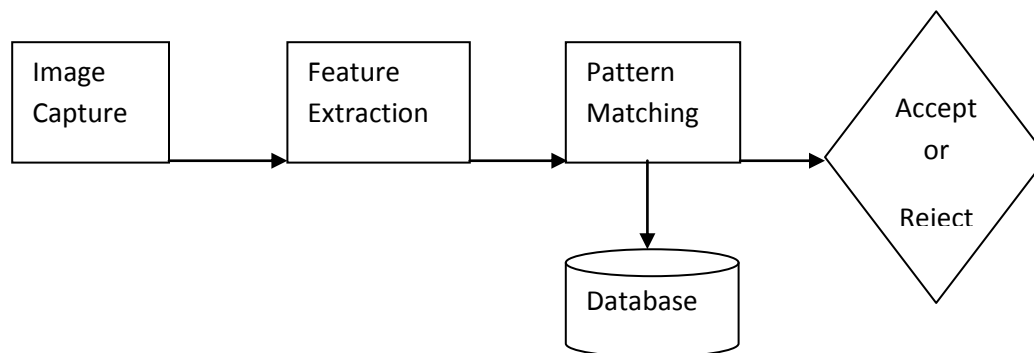


Fig. 1 Biometric finger print system ^[1]

Vaclav Matyas and Zdenek Riha et al

Explained in his paper the opinions about the usability of biometric authentication systems and secondly introduce a more systematic view of the process of biometric authentication – a layer model (of the biometric authentication process) which is related with the proposed model as biometric authentication is used in it.

He explained that firstly the image is acquired by image acquisition method through finger print module afterwards biometric measurements are processed and then the number of biometric samples necessary for further processed. After processing the biometric sample and extracting the features, the newly obtained master templates have to be stored. As soon as the user is enrolled, the user can use the system for successful authentications or identifications. Current biometric measurements must be obtained for the system to be able to make comparison with the master template. These subsequent acquisitions of the user's biometric measurements are done at various places where authentication of the user is required. The biometric measurements obtained in the previous step are processed and new characteristics are created. Currently computed characteristics are compared with the characteristics obtained during enrolment. If the system performs (identity) verification then these newly obtained characteristics are compared only to the master template. The final step in the verification process is the yes/no decision based on a threshold. This security threshold is either a parameter of the matching process or the resulting score is compared with the threshold value [2].

Neha Chaudhary et al gives the version of security device which consists of optical fibre link using biometric security at transmitter end and a code lock security at the receiver end. This proposed system is designed by keeping in mind the importance of security required for any communication system. She explained that, the data can only be transmitted by an authorized person and can only be received only when the password is known. She explained different methods and techniques which can be used to identify a person through its fingerprint. These mentioned methods conclude that the fingerprint is fast and accurate for more reliable and secure system. The methodology of the biometric identification system is represented with the help of diagrams and flow charts which can be used to enhance the quality of the image as well as to verify the identity of a person. Future research work can be carried out to improve the quality of the image by improving the image enhancement technique and develop a better matching technique [3].

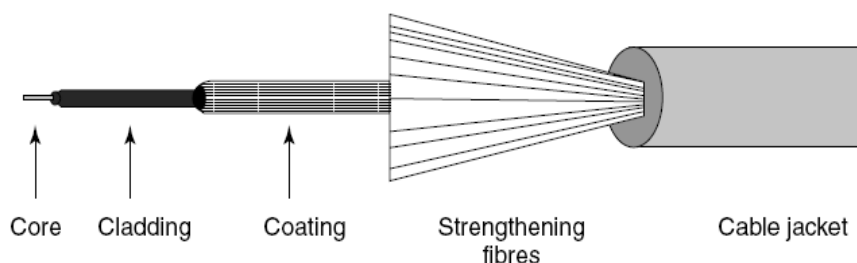


Fig.2 Internal view of optical fibre ^[3]

The authentication method used here is a four digit numeric code which is entered through the keypad. The code entered this way is then compared to the password stored in memory. The microcontroller continuously monitors the keypad for a match with the stored password. As and when there is a match the output line is enabled which can then be used to trigger an LED. A buzzer is triggered if the entered code doesn't match the stored password, as an audio indication that the lock has not been opened. An LCD display is also used to display whether the entered password is correct or not.

Annie P.oomen et al explained the idea to create a micro-controller based Digital Code Lock that serves the purpose of security. In the proposed model digital code lock is used at the receiver end. The digital code lock consists of microcontroller i.e.at89s52 as an access control system that allows only authorized persons to access a restricted area. The transmission and reception of data can only be done when the entered password is correct [4].

Adamu Murtala Zungeru et al

Through his paper he draws the attention to find a permanent solution to the increasing rate of crime, attacks by thieves, intruders and vandals, despite all security gadgets, locks by his electronic code lock technology. In this technology there is a great need of such type of locks for secure communication. The design procedure for the electronic combination lock consists of the power supply unit, the input, control and the output unit. The input unit comprises mainly of the keyboard and its switches each can generate a discrete signal when processed. When a key is pressed, the control unit receives signals from the input unit and processes them. The input unit is keypad used for entering the password. The control unit in the proposed model is microcontroller at89s52 and the output unit is the LCD screen which provides indication of authorized user to receive information [5].

Prachi Sharma et al provided an overview of optic fibre communication. And this paper is related to a greater extent with the proposed technology as optical fibre is chosen as a medium between transmitter and receiver for the communication of data in a secure manner. With the study of this paper optical fibre is best preferred to be used for both analog and digital data transmission and reception because of several properties like higher bandwidth, low losses and most important is security in transmission. This research paper is related with the proposed model as its study helps to know about various modes of optical fibre, the advantages of optical fibre, optical sources and due to this reasons the signals degrade in an optical fibre [6].

Shubham Pandey et al mentioned the uses and advantages of optical fiber link. He explained how an optical link can be used to transmit the data at a faster rate and in a secure manner. Also he explained that a biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode.

MODES OF PROPOSED SYSTEM

The proposed system can be classified into these modes-

□ **Biometric:**

- 1) Data base mode: In this mode we make the database of users in system.
- 2) Valid casting mode: In this mode we caste the finger. During casting the finger system automatically check the condition of finger. Is valid or not.
- 3) Checking mode: In this mode we check the status of valid finger or not valid finger. According to condition it operates the gate and provides alerting vision.

□ **Optical Link Mode:**

In this mode we use optical fiber for communication purpose. In this project we demonstrate the different idea of communication such as:

- 1) Voice communication: we send the analog signal in form of voice.
- 2) Data communication: for the data communication we use keypad and with the help of keypad we send the numeric data with the optical fibre channel.
- 3) Control mode: in control mode we provide automation concept by optical fibre with advance security.
- 4) Fail mode of optical link: in case of fault condition system check the status of optical link if any problem exist in optical communication system then system provide proper intimation.

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

□ **Automation:** As the name suggests for getting something done automatically. In this project proposal we will try to achieve automation at the receiver end and get it done from the transmitter end [7].

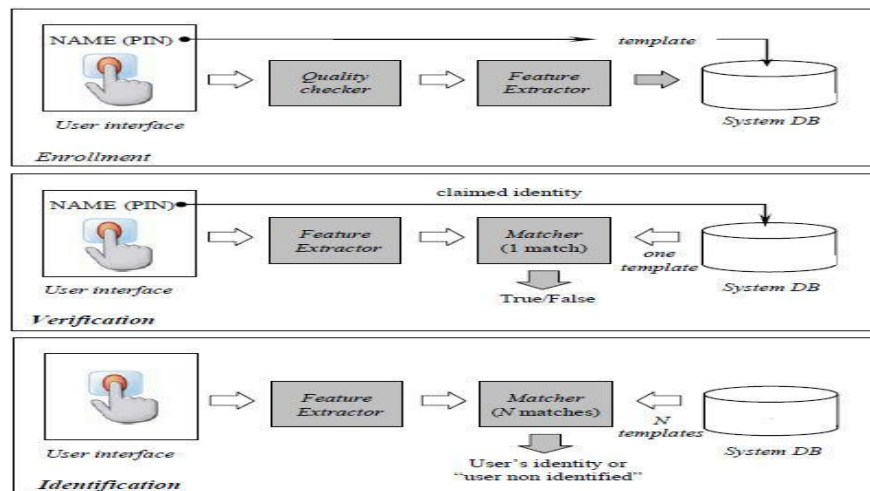


Fig.3. Block diagram of a Biometric System [7]

Priyanka Rani et al

In her paper she defines the various aspects and methods to be used for the fingerprint-based identification system. In the proposed model biometric authentication method i.e. finger print scanner is used as security module so, how the preset thumb prints are matched with the user thumb print who want to use transmit data from one end to the other. The proposed model is related with this technology for the image processing as firstly image is captured by finger print scanner and then image is filtered, segmented and then image enhancement is performed and finally finger print matching is done. A fingerprint is defined by a set of ridge lines and they run parallel and sometimes terminate and sometimes intersect. The points are known as Minutiae where the ridge lines are terminated, whereas according to Galton, each ridge is characterized by numerous minute peculiarities called Minutiae, which may divide and almost immediately reunite, enclosing a small circular or elliptical space or sometimes the independent beginning or ending of ridges. In a fingerprint image, ridges are dark whereas valleys are bright. Ridges and valleys often run in parallel, sometimes they bifurcate and sometimes they

terminate. Minutiae based fingerprint identification system approaches towards extraction of the ridge patterns correctly [8].

Mable P.Fok et al in the first part of his paper, he discussed various types of security threats that could appear in the optical layer of an optical network, including jamming, physical infrastructure attacks, and interception. Intensive research has focused on improving optical network security, in various areas where there is a great need of secure communication. Real-time processing of the optical signal is essential in order to integrate security functionality at the physical layer while not undermining the true value of optical communications, at a very high speed using optical fiber. Optical layer security benefits from the unique properties of optical processing-instantaneous response, broadband operation, electromagnetic immunity, compactness, and low latency. In the second part of his paper, various defenses against the security threats outlined in this paper are discussed, including optical encryption, optical code-division multiple access (CDMA) confidentiality, self-healing survivable optical rings and anti-jamming. These properties of optical fiber can be used for fast and secure communication so that the data we are transmitting may be received in the same form as we have transmitted and there is no loss of any information [9].

3. PROBLEM IDENTIFICATION

Communication is an important part of our daily life. The communication process involves information generation, transmission, reception and interpretation. A technical overview of the emerging technologies of fibre optical communication and optical networking fibre optical communications has enabled much higher data rates. In present scenario, it is continuously being noticed that people are very concerned about privacy of their data. But some unauthorized persons, who are aware of technology, can access other's data. So to provide security to the people for their data multiple security systems are being used in the present scenario like biometric which is well known for being used in the security purpose and second one is optical fibre link which is also used for the security purpose. Other security systems are code lock, RF-ID etc. So in present scenario the biggest problem is to provide security where secure communication is required such as bank, industry, college and election commission etc.

Through this system analog and digital data can be transmitted using highly secured optical fibre link while having a biometric security to transmit the data at the transmitter end and having a code lock security for reception purpose at the receiver end. Through this project automation can also be done at the receiver end from

the transmitter end. In this system we demonstrate the idea of security for valid and invalid person. If any person wants to enter in any secured region, system will demand finger ID. If ID is valid, only then system will provide access through optical link between transmitter and receiver section. In case of invalid ID, system will automatically check the status and beep the buzzer and close the optical link between transmitter and receiver section.

4. DESIGN AND IMPLEMENTATION OF PROPOSED SYSTEM

Block diagram of proposed system is shown in fig. The heart of the circuit is microcontroller at89s52. Other components used are voltage regulator7805, LCD display 16x2, matrix keypad, relay, buzzer, and finger print scanner. First of all, to take 220V that from ac terminal step down transformer convert into 12V and capacitor use to reduce the harmonics that introduce during rectification. And regulator 7805 IC provides fixed five volts. The database is entered with the help of keypad and fingerprint scanner and all condition display in LCD. If someone wants to send the data and voice with the proposed system, it demands for finger touch and then the system match it with the fingerprint stored in database and operate the relay in case of valid finger and allow for communication voice and data.

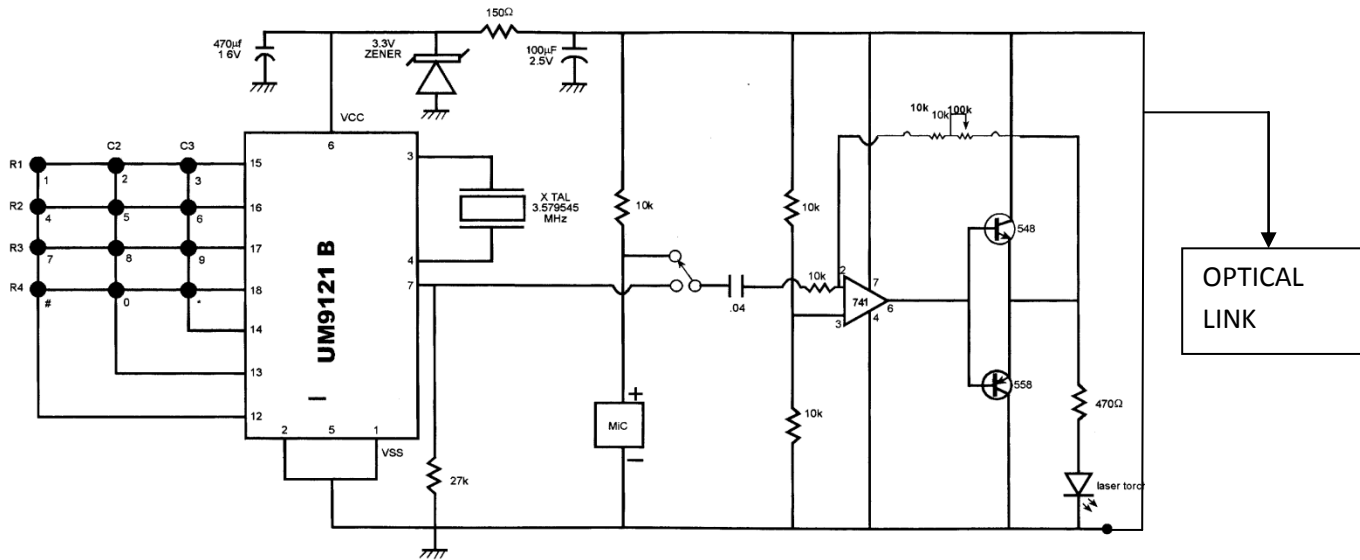


Fig.5 Transmitter circuit

WORKING OF TRANSMITTER

With this system two signals one is digital and second signal from mike can be sent. Change over switch is used to select the signals. Data is fed from mike, then mike convert the audio signal into electrical signal and this electrical signal is coupled to the pin no 2 at I.C 741. Here I.C 741 is used as a mike amplifier. Pin no 7 is connected to the voltage at pin no4 is connected to the negative voltage at pin no6 is output pin. Amplified output is available on pin no6. For further amplification, transistor circuit is used. Output of Transistor circuit is connected to the laser light. Actual signal from transistor circuit is converted into light. Zener diode is used with laser light to protect them from high voltage. Data is now superimposed on the laser light and this laser light is focused on thereceiver. At receiver side photo sensor is used and when laser light focus on the photo sensor the photo sensor convert this light into voltage, this Small voltage in the farm at signals is again fed to the pin no2 at I.C 741. Again Amplified output available on pin no6 at I.C741 and further Amplified by a transistor circuit.

In the digital transmission, transfer of data is in digital form. In digital form one numeric keyboard is used at transmitter and at the receiver section one numeric display circuit is used. In transmitter section 9 switches are used for the nine decimal numbers and at the output circuit seven segment displays is used for the numeric display.

5. RESULT AND DISCUSSION

The result of transmitter circuit is that it generates optical input and that optical input is transferred through optical link and a photo sensor is used at the receiver's end which detects optical output and it converts the optical signal into electrical signals. And further the system demands for entering the password in case user wants to receive whatever data is transmitted through the transmitter.

The result of this complete description is that by using this advance and intelligent optical link system the data can be transmitted and received only through an authorized person no other person can send and receive the data through this link and hence security is taken into major consideration.

6. CONCLUSION

The conclusion of whole description is that work can be done upon implementing the idea of advance biometric based security system. This technique will be very useful for college/bank/other imported place and election commission. By working upon this more advancement can be achieved in security system and can automatically control different appliances from one place without any movement. The user may be authenticated by a finger print system to confirm access. And the digital lock used at the receiver side is able to implement all the functions specified in our proposal.

As the result of study of research papers on different security technologies an intelligent system using optical fibre is proposed that can be used for highly secured communication and same optical link can be used for automation. Fingerprint module provides higher security for the data transmission [2].

7. FUTURE SCOPE

Fibre optics communication is definitely the future of data communication. The evolution of fibre optic communication has been driven by advancement in technology and increased demand for fibre optic communication. It is expected to continue into the future, with the development of new and more advanced communication technology. The fibre optics communications industry is an ever evolving one, the growth experienced by the industry has been enormous this past decade. There is still much work to be done to support the need for faster data rates, advanced switching techniques and more intelligent network architectures that can automatically change dynamically in response to traffic patterns and at the same time be cost efficient. The trend

is expected to continue in the future as breakthroughs already attained in the laboratory will be extended to practical deployment thereby leading to a new generation in fibre optics communications.

8. REFERENCES

1. Ravi subban “A Study of Biometric Approach Using Fingerprint Recognition”, Vol. 1, No. 2, May 2013.
2. Vaclav Matyas and Zdenek Riha, “Biometric authentication-security and usability”, Faculty of Informatics, Masaryk University Brno, Czech Republic.
3. Neha Chaudhary, Sangeeta Singh, Shivani Gupta and Shubham Pandey, “A Review Paper on Optical Communication using Biometric and Code lock”, Published in Imperial Journal of Interdisciplinary Research, volume-2, Issue -11, 2016.
4. Annie P.O 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, Volume- 3, Issue 2, February 2014.
5. 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.
6. Prachi Sharma, Rohit kumar, Arora, Suraj Pardeshi and Mandeep Singh, “Fibre Optic Communication : An Overview”, Published in International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 5, May 2013.
7. Shubham Pandey, Shivani Gupta, Neha Chaudhary and Sangeeta Singh, “Study of a Secure Communication”, Published in Imperial Journal of Interdisciplinary Research, volume-2, Issue-11, 2016.
8. Priyanka Rani, Pinki Sharma, “A Review paper on Finger Print Identification system” Published in International Journal of Advanced Research in Computer Science & Technology IJARCST 2014, Volume- 2, Issue 3 July - Sept. 2014.
9. Mable P. Fok “Optical Layer Security in Fibre Optic Networks” published in IEEE Transactions on Information Forensics and Security Volume- 6, Issue 3, 2011.
10. 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.

11. Umut Uludaga, Arun Rossb, Anil Jain, "Biometric template selection and update: a case study in Fingerprint Recognition." in Proc. IEEE 1991 International Symposium on CAS, Singapore, in 1991.
12. Md. Mahbubur Rahman, Amit Karmaker, Md. Mahmudul Hasan and Samsuddin Ahmed, "Ensuring Quality in Biometric Systems" Published in International Journal of Security and Its Applications Volume- 9, No. 4 2015.
13. Asker M. Bazen, Gerben T.B. Verwaaijen, Sabih H.Gerez, "A Correlation-Based Fingerprint Verification System." Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands, November 2000.
14. Francis Idachaba, Dike U. Ike and Orovwod Hope, "Future trends in fibre optic communication", Proceedings of the World Congress on Engineering 2014 Volume-1, WCE 2014, July 2, 2014, London, U.K.
15. Renu Bhatia, "Biometrics and face recognition techniques" Published in International Journal of Advanced research in computer science and software engineering Volume- 3, Issue 5, 2013.
16. Pulkit Berwal, "Development in the Field of Optical Fibre Communication Systems: A Review", Published in International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS) Voume-2, Issue 01, December 2013.
17. Ritesh A. Jadhav, Dattatraya S. Shitole, "Fibre Optics Communications and Applications" published in Intrenational Journal of Innovative Research in Engineering and Science, ISSN 2319-5665, issue 2, volume 4, April 2013.

9. ABOUT AUTHORS

Sangeeta Singh is pursuing B.Tech in Electronics & Communication Engineering from Moradabad Institute of technology, Moradabad. Area of interest includes Communication, Embedded system, Wireless Technology.

Ruchi Varshney is having a great experience in the field of academics for 14 years and presently working as an assistant professor, Dept. of E&C Engg., at MIT Moradabad. She has published number of papers in National and International Journals and Conferences.

Neha Chaudhary is pursuing B.Tech in Electronics & Communication Engineering from Moradabad Institute of technology, Moradabad. Area of interest includes Communication, Embedded system, Wireless Technology.

Shubham Pandey is pursuing B.Tech in Electronics & Communication Engineering from Moradabad Institute of technology, Moradabad. Area of interest includes Communication, Embedded system, Wireless Technology.

Shivani Gupta is pursuing B.Tech in Electronics & Communication Engineering from Moradabad Institute of technology, Moradabad. Area of interest includes Communication, Embedded system, Wireless Technology.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper, Summary of Research Project, Theses, Books and Book Review for publication.

**Address:- North Asian International Research Journal Consortium (NAIRJC)
221, Gangoo Pulwama - 192301**

Jammu & Kashmir, India

Cell: 09086405302, 09906662570,

Ph No: 01933212815

Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com

Website: www.nairjc.com

