Smart Intelligent ATM Using LABVIEW

M.Padmavathi[1], R.Nagarajan [2]
[1]Assistant Professor, Department of Electrical and Electronics Engineering, Gnanamani College of Technology, Namakkal, Tamil Nadu, India.
[2]Professor, Department of Electrical and Electronics Engineering, Gnanamani College of Technology, Namakkal, Tamil Nadu, India.

Abstract – Now a day, peoples have multiple bank accounts so money transactions play a vital role in the nature of trade. Today, ATMs (Automated Teller Machine) and credit cards are used for this purpose, the authentication of these transactions are unsecure. To overcome this shortcoming of money transactions, we proposes the idea of using fingerprints of customers as login multiple banking password in place of traditional PIN (Personal Identification Number) number. Here, if the fingerprint is recognized, then it displays the multiple banking screens. The customer can choose the bank which we need for transaction. The remaining feature are same as i.e., a reference fingerprint of the nominee or a close family member of the customer can be used if the customer is not available in case of emergencies. This proposed business model helps the society, mainly the rural people, by enhancing the security using fingerprint recognition in digital image processing. As the fingerprint of every person is unique and unchangeable, this biometric feature is used over the others.

Index Terms – ATM - Automated Teller Machine, PIN - Personal Identification Number, Ttransactions, Authnetication, Biometric.

1. INTRODUCTION

The ATM is an automated teller machine which is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller. In ATMs the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smartcard with a chip that contains a unique card number and some security information. The first ATM was installed in Enfield town in London on June 27, 1967 by Barclays Bank. The ATMs are known by various other names as Automated Transaction Machine, Automated Banking Machine, Cash Point (at Britain), Hole in the wall, Ban comet (in Europe and Russia) and Any Time Money (in India) [1].

Some people used to write their PIN and password on some paper or diary which is not at all secure. As, it can be easily attacked and hacked by someone, resulting the account holder can suffer. With the growing sector of banking, everyone is using ATM machines as these machines are located in different places and the customer can access his account anytime anywhere. A customer holding a bank account can access the account from ATM systems by getting a PIN or password confidentially [2].

Although various biometric technique like- fingerprint, eye recognition, retina and iris recognition, etc have been devised as an authentication method for ATM machines, still there is need to enhance the security in ATM systems to overcome various challenges. The biometrics is a technology that helps to make your data tremendously secure, distinguishing all the users by way of their personal physical characteristics. The biometric information can be used to accurately identify people by using their fingerprint, voice, face, iris, handwriting, or hand geometry and so on. Using biometric identifiers offers several advantages over traditional and current methods [3]. Tokens such as magnetic stripe cards, smart cards and physical keys, can be stolen, lost, duplicated, or left behind; passwords can be shared, forgotten, hacked or unintentionally observed by a third party. There are two key functions offered by a biometric system. One method is identification and the other is verification [4].

In this paper, we are concentrating on identifying and verifying a user by fingerprint recognition. The modern ATM is typically made up of the devices like CPU to control the user interface and devices related to transaction, Magnetic or Chip card reader to identify the customer, PIN Pad, Secure crypto processor generally within a secure cover. The display to be used by the customer for performing the transaction, Function key buttons, Record Printer to provide the customer with a record of their transaction, to store the parts of the machinery requiring restricted access - Vault, Housing for aesthetics, Sensors and Indicators [5].

The fingerprint technology is the most widely accepted and mature biometric method and is the easiest to deploy and for a higher level of security at your fingertips. It is simple to install and also it takes little time and effort to acquire one's fingerprint with a fingerprint identification device [3]. Thus, fingerprint recognition is considered among the least intrusive of all biometric verification techniques. Ancient time's officials used thumbprints to seal documents thousands of years ago, and law agencies have been using fingerprint identification since the late 1800s. We here carry the same technology on digital platform. Although fingerprint images are initially captured, the images are not stored anywhere in the system. Instead, the fingerprints are converted to templates

from which the original fingerprints cannot be recreated; hence no misuse of system is possible [6].

The fingerprint based ATM is a desktop application where fingerprint of the user is used as an authentication. The finger print minutiae features are different for each human being so the user can be identified uniquely. Instead of using ATM card fingerprint based ATM is safer and secure. There is no worry of losing ATM card and no need to carry ATM card in your wallet. You just have to use your fingerprint in order to do any banking transaction [7].

2. BIOMETRICS

The biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face, fingerprint, hand geometry, iris, retinal, signature, and voice. The biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent [8].

The biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives. This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it Provides for positive authentication), can provide an audit trail and is becoming socially acceptable and inexpensive [9].

The biometrics technologies verify identity through characteristics such as fingerprints, voices, and faces. By providing increased security and convenience, biometrics has begun to see widespread deployment in network, e-commerce, and retail applications. This book provides in-depth analysis of biometrics as a solution for authenticating employees and customers [10].

Figure 1 Fingerprint Scanner

Humans recognize each other according to their various characteristics for ages. We recognize others by their face when we meet them and by their voice as we speak to them. Identity verification (authentication) in computer systems has been traditionally based on something that one has (key, magnetic or chip card) or one knows (PIN, password) [11]. The Figure 1 shows the fingerprint scanner of the biometrics system.

The biometric systems can be used in two different modes. Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the verification biometric data obtained from the user is compared to the user's data already stored in the database. Identification (also called search) identification occurs when the identity of the user is a priori unknown.

The biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information [12].

A fingerprint scanner system has two basic jobs -- it needs to get an image of your finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images. The situation improves as these systems spread around and become more common. Systems that can automatically check details of a person's fingerprint have been in use since the 1960s by law enforcement agencies. The U.S. Government commissioned a study by Sandia Labs to compare various biometric technologies used for identification in early seventies.

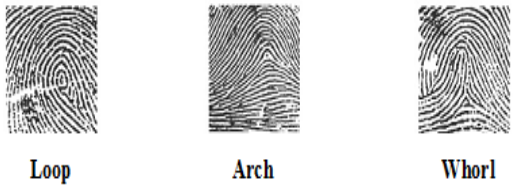

Figure 2 Step by Step Processes

The nutiae are individual unique character minutiae istics within the fingerprint pattern such as ridge endings, bifurcations, divergences, dots or islands (see the picture on the following page). The correlation-based method is able to correlation overcome some of the difficulties of the minutiae-based approach. Based however, it has some of its own shortcomings. Correlation based techniques require the precise location of a registration point and are affected by image

translation and rotation [5]. Source: Digital Persona the loop is the most common type of fingerprint pattern and accounts for about 65% of all prints. The readability of a fingerprint depends on a variety of work and environmental factors. These include age, gender, occupation and race. The Figure 2 shows the Step by Step processes of the biometrics system.

In today's criminal justice applications, the AFIS systems achieve over 98% identification rate while the FAR is below 1%. The typical access control systems, on the other side, are completely automated. Their accuracy is slightly worse. The quality of the fingerprint image obtained by an automated fingerprint reader from an inexperienced (non-professional) user is usually lower. Device-independent software is not bound to images obtained by one single input device, but their accuracy is very low if various input devices are mixed. Source: PRIP MSU the minutiae matching is a process where two sets of minutiae are compared to decide whether they represent the same finger or not [13] . Figure 3 shows the multiple input biometrics system.

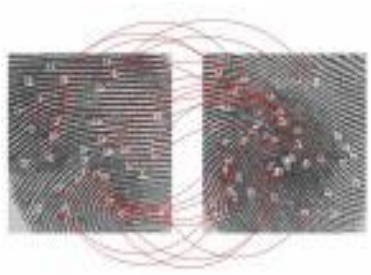

Figure 3 Multiple Input Biometrics System

There are five stages involved in finger scan verification and identification. Fingerprint (FP) image acquisition, image processing, and location of distinctive characteristics, template creation and template matching. A scanner takes a mathematical snapshot of a user's unique biological traits. This snapshot is saved in a fingerprint database as a minutiae file. The first challenge facing a finger scanning system is to acquire high quality image of a fingerprint. The standard for forensic quality fingerprinting is images of 500 dots per inch (DPI) [8], [9]. Image acquisition can be a major challenge for finger scan developers, since the quality of print differs from person to person and from finger to finger. Some populations are more likely than others to have faint or difficult-to-acquire fingerprints [14], whether due to wear or tear or physiological traits. Taking an image in the cold weather also can have an affect. Oils in the finger help produce a better print. In cold weather, these oils naturally dry up. Pressing harder on the platen (the surface on which the finger is placed, also known as a scanner) can help in this case. Image processing is the process of converting the finger image into a usable format. This results in a series of thick black ridges (the raised part of the fingerprint) contrasted to white valleys [10].

3. HARDWARE DESIGN

The Figure 4 shows the block diagram of fingerprint based ATM. The block diagram of the proposed system and design aspects of independent modules are considered. Hardware is essential to any embedded system. Figure 1 shows the block diagram of the fingerprint based ATM authentication system. The main blocks of this system are: (i) Regulated Power Supply, (ii) PIC 16F877A Microcontroller, (iii) Fingerprint Module, (iv) Liquid Crystal Display and (v) Buzzer [15], [16].

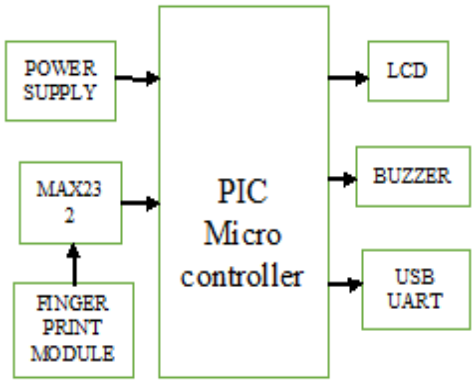

Figure 4 Block Diagram of Fingerprint Based ATM

The PIC16F877A CMOS FLASH-based 8-bit microcontroller is upward compatible with the PIC16C5x, PIC12Cxxx and PIC16C7x devices. It features 200 ns instruction execution, 256 bytes of EEPROM data memory, self-programming, an ICD, 2 Comparators, 8 channels of 10-bit Analog-to-Digital (A/D) converter, 2 capture/compare PWM functions [17], a synchronous serial port that can be configured as either 3-wire SPI or 2-wire I2C bus, a USART, and a Parallel Slave Port [18].

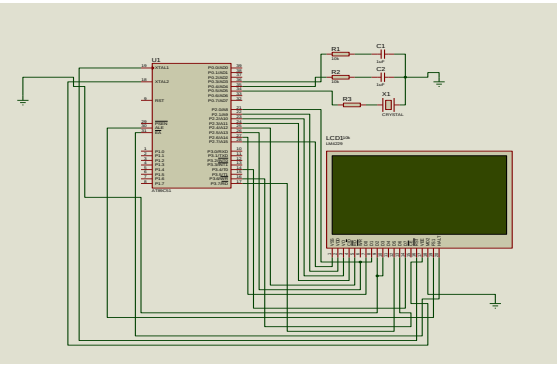

Figure 5 Circuit Diagram of Fingerprint Based ATM

The data in the register RSR, the information is loaded at the same time into the register RCREG. Obviously, using 2 registers allows faster receiving of the data. While the information that was received being transferred into RCREG, the new information has already been received into the register

RSR. Of course, the CREN bit needs to be set. According to the USART TRANSMIT / RECEIVE block diagram, that the information that was transmitted via pin RC6 in Port C, is received through the pin RC7 in Port C [19], [20]. The Figure 5 shows the circuit diagram of the fingerprint based ATM. The liquid crystal display (LCD) is used to display the results of the system operation such as sensed values, motor status etc…A LCD is a flat panel display, electronic visual display, or video display that uses the light modulating properties of liquid crystals. Liquid crystals do not emit light directly. The LCD standard requires 3 control lines and 8 I/O lines for the data bus [21].

The most commonly used Character based LCDs are based on Hitachi's HD44780 controller or other which are compatible with HD44580. In this tutorial, we will discuss about character based LCDs, their interfacing with various microcontrollers, various interfaces (8-bit/4-bit), programming, special stuff and tricks you can do with these simple looking LCDs which can give a new look to your application [22].

There are two 8-bit registers in HD44780 controller Instruction and Data register. Instruction register corresponds to the register where you send commands to LCD e.g LCD shift command, LCD clear, LCD address etc. and Data register is used for storing data which is to be displayed on LCD. when send the enable signal of the LCD is asserted, the data on the pins is latched in to the data register and data is then moved automatically to the DDRAM and hence is displayed on the LCD [23], [24]. Data Register is not only used for sending data to DDRAM but also for CGRAM, the address where you want to send the data, is decided by the instruction you send to LCD. We will discuss more on LCD instruction set further in this tutorial [25]-[27].

4. LABVIEW

Laboratory Virtual Instrument Engineering Workbench (LabVIEW) is a system design platform and development environment for visualprogramming language from the National Instruments. LabVIEW integrates the creation of user interfaces (termed front panels) into the development cycle. LabVIEW programs-subroutines are termed virtual instruments (VIs). The graphical approach also allows nonprogrammers to build programs by dragging and dropping virtual representations of lab equipment with which they are already familiar [19]. Each VI has three components: a block diagram, a front panel, and a connector panel. The last is used to represent the VI in the block diagrams of other, calling VIs. The front panel is built using controls and indicators. The front panel serving as a user interface, or, when dropped as a node onto the block diagram, the front panel defines the inputs and outputs for the node through the connector panel. This implies each VI can be easily tested before being embedded as a subroutine into a larger program.

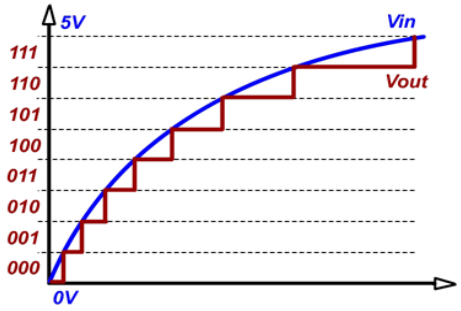

Figure 4 LabVIEW Output

The LabVIEW programming environment, with the included examples and documentation, makes it simple to create small applications. This is a benefit on one side, but there is also a certain danger of underestimating the expertise needed for high quality programming [16]. For complex algorithms or large scale code, it is important that a programmer possess an extensive knowledge of the special LabVIEW syntax and the topology of its memory management. The most advanced LabVIEW development systems offer the ability to build stand-alone applications [21]. The LabVIEW software in PC consists of database of customer and bank account details. It consists about the accounts hold by the costumer. It matches the digital information obtained from the microcontroller through USB and UART, and compares those signals with database available in PC [28], [29].

5. CONCLUSION

This paper presented a prototype design of an ATM access system using fingerprint technology. The system consists of fingerprint module, DC motor and LCD display. These are interfaced to the PIC microcontroller. When a user registers his fingerprint to the fingerprint scanner module, this is fed as input to the microcontroller. The microcontroller is programmed in such a way that the input from. When a authorized person is recognized using fingerprint scanner module the door is accessed using DC motor. The finger scan technology is being used throughout the world and provides an able solution. The system can be extended using a GSM module. The GSM module sends alert messages to the respective authorities when unauthorized person's finger print is detected.

REFERENCES

[1] Archana et al., "Enhance the Security in the ATM System with Multimodal Biometrics and Two-Tier Security", International Journal of Advanced Research in Computer Science and Software Engineering 3(10), pp. 261-266, October – 2013.

[2] S.T. Bhosale and Dr. B.S.Sawant "Security in E-Banking via Card Less Biometric ATMs", International Journal of Advanced Technology & Engineering Research, Volume 2, Issue 4, July 2012

[3] J.Chandramohan, R.Nagarajan, K.Satheeshkumar, N.Ajithkumar, P.A.Gopinath and S.Ranjithkumar, "Intelligent Smart Home Automation and Security System Using Arduino and Wi-fi,"

International Journal of Engineering And Computer Science (IJECS), Volume 6, Issue 3, pp. 20694-20698, March, 2017.
[4] Sunil Lohiya "Biometric identification and verification techniques -A future of ATM Banking System", Indian Streams Research Journal, Volume 2, Issue. 7, Aug 2012
[5] *G. Vidhya Krishnan, R.Nagarajan, T. Durka, M.Kalaiselvi, M.Pushpa and S. Shanmuga priya,* "Vehicle Communication System Using Li-Fi Technology," International Journal of Engineering And Computer Science (IJECS), Volume 6, Issue 3, pp. 20651-20657, March, 2017.
[6] Ms. C. Hemalatha, Mr. R. Nagarajan, P. Suresh, G. Ganesh Shankar and A. Vijay, "Brushless DC Motor Controlled by using Internet of Things," IJSTE - International Journal of Science Technology & Engineering, Volume -3.Issue-09, pp. 373-377, March- 2017.
[7] Biswas S., Bardhan Roy A., Ghosh K. And Dey N.,"A Biometric Authentication Based Secured ATM Banking System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012
[8] S.Suresh, R.Nagarajan, L.Sakthivel, V.Logesh, C.Mohandass and G.Tamilselvan, "Transmission Line Fault Monitoring and Identification System by Using Internet of Things," International Journal of Advanced Engineering Research and Science (IJAERS), Vol-4.Issue-4, pp. 9-14, Apr- 2017.
[9] R.Nagarajan, R.Yuvaraj, V.Hemalatha, S.Logapriya, A.Mekala and S.Priyanga, "Implementation of PV - Based Boost Converter Using PI Controller with PSO Algorithm," International Journal of Engineering And Computer Science (IJECS), Volume 6, Issue 3, pp. 20479-20484, March, 2017.
[10] Dr.R.Nagarajan, S.Sathishkumar, K.Balasubramani, C.Boobalan, S.Naveen and N.Sridhar. "Chopper Fed Speed Control of DC Motor Using PI Controller," IOSR- Journal of Electrical and Electronics Engineering (IOSR-JEEE), Volume 11, Issue 3, Ver. I, pp. 65-69, May – Jun. 2016.
[11] Zahid Riaz, Suat Gedikli, Micheal Beetz and Bernd Radig "A Uni_ed Features Approach to Human Face Image Analysis and Interpretation", 85748 Garching, Germany
[12] J.Chandramohan, R.Nagarajan, M.Ashok kumar, T.Dineshkumar, G.Kannan and R.Prakash, "Attendance Monitoring System of Students Based on Biometric and GPS Tracking System," International Journal of Advanced Engineering, Management and Science (IJAEMS), Vol-3.Issue-3, pp. 241-246, Mar. 2017.
[13] K. Anandhi and Dr. R. Nagarajan, "Mutex-Heart: Fail Safe Dual Chamber Cardiac Pacemaker Device with Rate Responsive Control and Cryptographic Security," IJSRD- International Journal for Scientific Research & Development. Vol. 3, Issue- 2, pp. 489-493, 2015.
[14] Edmund Spinella SANS GSEC," Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", San Francisco, 28 May 2003.
[15] R.Nagarajan and M,Saravanan. "Performance Analysis of a Novel Reduced Switch Cascaded Multilevel Inverter," Journal of Power Electronics, Vol.14, No.1, pp. 48-60, Jan.2014.
[16] R.Nagarajan, S.Sathishkumar, S.Deepika, G.Keerthana, J.K.Kiruthika and R.Nandhini, "Implementation of Chopper Fed Speed Control of Separately Excited DC Motor Using PI Controller", International Journal of Engineering And Computer Science (IJECS), Volume 6, Issue 3, pp. 20629-20633, March, 2017.
[17] R.Nagarajan and M, Saravanan, "A Carrier - Based Pulse Width Modulation Control Strategies for Cascaded Multilevel Inverter", International Review on Modeling and Simulations, Vol.6. No.1, pp. 8-19. Feb 2013.
[18] C.Mallika devi and R.Nagarajan, "High-Power Transformer-Less Wind Energy Conversion System with three phase Cascaded Multilevel Inverter," International Journal of Scientific & Engineering Research. Vol. 4, Issue- 5, pp. 67-70, May-2013.
[19] R.Nagarajan, A.Mahendran and K.Muthulakshmi, "Triangular Multicarrier SPWM Technique for Nine Level Cascaded Inverter," International Journal of Scientific & Engineering Research, Vol.4, No.5, pp. 269-275, May-2013.
[20] Aru, Okereke Eze, Ihekweaba Gozie," Facial Verification Technology for Use In ATM Transactions", American Journal of Engineering Research (AJER), Volume-02, Issue-05, pp-188-193
[21] R.Nagarajan and M,Saravanan "Staircase Multicarrier SPWM Technique for Nine Level Cascaded Inverter," 2013 International Conference on Power, Energy and Control (ICPEC), IEEE Press, pp-668-675. 2013.
[22] R.Nagarajan, J.Chandramohan, R.Yuvaraj, S.Sathishkumar and S.Chandran, "Performance Analysis of Synchronous SEPIC Converter for a Stand-Alone PV System," International Journal of Emerging Technologies in Engineering Research (IJETER), Vol. 5, Issue - 5, pp. 12-16, May-2017.
[23] R Rameshkumar and R Nagarajan, "Sine Multicarrier SPWM Technique for Seven Level Cascaded Inverter," CiiT-Programmable Device Circuits and Systems. Vol. 5, Issue- 6, 2013.
[24] R.Nagarajan and M, Saravanan, "Comparison of PWM Control Techniques for Cascaded Multilevel Inverter" International Review of Automatic control (IRACO), Vol.5, No.6, pp. 815-828. Nov. 2012.
[25] M. Pantic and L.J.M. Rothkrantz," Facial gesture recognition in face image sequences: A study on facial gestures typical for speech articulation", P.O. Box 356, 2600 AJ Delft, The Netherlands
[26] R.Nagarajan, J.Chandramohan, S.Sathishkumar, S.Anantharaj, G.Jayakumar, M.Visnukumar and R.Viswanathan, "Implementation of PI Controller for Boost Converter in PV System," International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE). Vol.11, Issue.XII, pp. 6-10, December-2016.
[27] Prof. Selina Oko and Jane Oruh, "ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012
[28] http://australianit.news.com.au/articles/0,7204,5633467%5E15397%5E%5E nbv%5E,00.html.
[29] Dr.R.Nagarajan, R.Yuvaraj. K.Dinesh Kumar, R.Dinesh Babu, M.Manikandan and S.Meiyanbu. "Implementation of SPWM Technique for Inverter," International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST). Vol. 2, Issue- 9, pp. 10-14. September 2016.

Authors

M.Padmavathi received her B.E. in Electrical and Electronics Engineering from Madras University, Chennai, India, in 2001. She received her M.E. in Power Electronics and Drives from Anna University, Chennai, India, in 2009. She has worked in the various institution as an Assistant Professor. She is currently working as a Assistant Professor of Electrical and Electronics Engineering at Gnanamani College of Technology, Namakkal, Tamilnadu, India.

R. Nagarajan received his B.E. in Electrical and Electronics Engineering from Madurai Kamarajar University, Madurai, India, in 1997. He received his M.E. in Power Electronics and Drives from Anna University, Chennai, India, in 2008. He received his Ph.D in Electrical Engineering from Anna University, Chennai, India, in 2014. He has worked in the industry as an Electrical Engineer. He is currently working as Professor of Electrical and Electronics Engineering at Gnanamani College of Technology, Namakkal, Tamilnadu, India. His current research interest includes Power Electronics, Power System, Soft Computing Techniques and Renewable Energy Sources.