Volume 3, No. 11, November 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

HIGH PROTECTION HUMAN IRIS AUTHENTICATION IN NEW ATM TERMINAL DESIGN USING BIOMETRICS MECHANISM

[1]Mr C Raghavendra [2]Dr S. Sivasubramanian [3]Dr A M Sameeullah
[1]Research Scholar, Dept. of CSE, Bharath University, Chennai.
[2]Professor, Department of IT, Dhanalakshmi College of Engg, Chennai.
drsivamdu2011@gmail.com
[3]Professor Department of CSE, Dhanalakshmi College of Engg, Chennai.

Abstract- For the traditional ATM terminal customer recognition systems only rely on bank cards, passwords, and such identity verification methods which measures are not perfect and functions are too single. For solving the bugs of traditional ones, using a Biological Technology in new ATM terminal customer recognition systems i.e., IRIS Biometrics Mechanism. A biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual**.** Using iris recognition in ATM a customer simply walks up to the ATM and looks in a sensor camera to access their accounts. The camera instantly photographs the iris of the customer. If the customers iris data matches the record stored a database access is granted. At the ATM, A positive authentication can be read through glasses, contact lenses and most sunglasses. The performance of the system is evaluated by using the number of degrees of freedom, False Reject Rate (FRR), False Accept Rate (FAR), and Equal Error Rate (EER) and the metrics show that the proposed algorithm can be employed for an high protection human iris recognition system.

INTRODUCTION

With the development of computer network technology and e-commerce, the self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. Nowadays, using the ATM (Automatic Teller Machine) which provide customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years, a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password can not verify the client's identity exactly. Biometrics deals with automated methods of recognizing a person based on physiological characteristics such as face, fingerprints, hand geometry, iris, retinal, and vein. Biometric authentication technique based on iris patterns is suitable for high level security systems. Iris is the annular ring between the pupil and the sclera of the eye.

The structure of iris is fixed from about one year in age and remains constant over time. It exhibits long-term stability and infrequent re enrolment requirements. The variations in the gray level intensity values distinguish two individuals. The difference exists between identical twins and even between left and right eye of the same person. As the technology is iris pattern-dependent, not sight dependent.

INGRAINING OF IRIS RECOGNITION IN ATM'S

The paper aims at developing a high protection iris recognition based biometric authentication scheme in ATM banking systems. It mainly reduces the accessing time, when compared with manual based banking system. ATM's are now a normal part of daily life, it explores the accessibility barriers that ATM.s present to people with a variety of disabilities, particularly examining the access barriers experienced by the people who are blind, vision impaired or who have reading, learning or
intellectual disabilities.

a. Stencil on Card (SOC). The biometric Stencil is stored on a hardware security module. It must be retrieved and transmitted to a different system that matches it to the live template acquired by special scanners from the user.
b. Match on Card (MOC). The biometric stencil is stored on a hardware security module, which also performs the matching with the live stencil.
Therefore, a microprocessor smartcard is necessary, which must be endowed with an operating system running suitable match applications.
c. System on Card (SOC). This is a combination of the previous two technologies. The biometric Stencil is stored on a hardware security module, which also performs the matching with the live stencil, and hosts the biometric scanner to acquire, select and process the stencil.

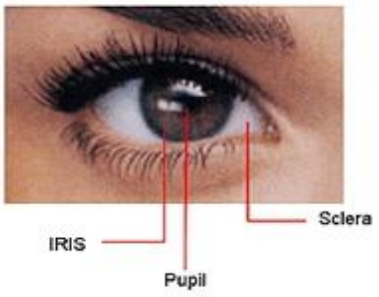
Basic Concept of IRIS:

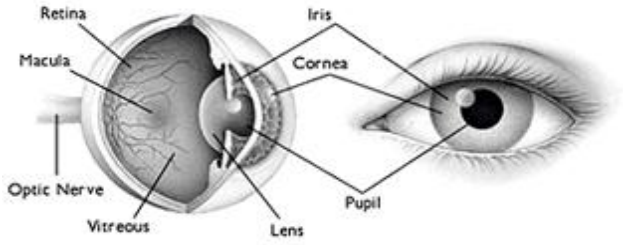
The human Iris is an internal organ of the eye, protected by the eyelid, cornea. The iris is the colored portion of the eye that surrounds the pupil .It controls light levels inside the eye similar to the aperture of a camera. The round opening in the center of the iris is called the pupil. The iris is embedded with tiny muscles that dilate and constrict the pupil size. The iris features remain constant throughout the years.

IRIS Recognition:

Iris recognition is a method of biometric

authentication that uses pattern recognition techniques based on high-resolution images of the iris of an individual's eyes. Iris systems have a very low False Accept Rate (FAR) compared to other biometric traits; the False Reject Rate (FRR) of these systems can be rather high. Image processing techniques can be employed to extract the unique iris pattern from a digitized image of the eye, and encode it into a biometric template, which can be stored in a database. This biometric stencil contains an objective mathematical representation of the unique information stored in the iris, and allows comparisons to be made between stencils.





Iris Recognition System:

A typical iris recognition system in involves three main modules:

a. Image acquisition:

It is to capture a sequence of iris images from the subject using a specifically designed sensor.

b. Preprocessing Stage:

It includes determining the boundary of the iris within the eye image, and extracts the iris portion from the image to facilitate its processing. It includes various stages such as:
a. Iris Segmentation
d. Iris Normalization
e. Image Enhancement

c. Feature extraction and Encoding:

This is the most key component of an iris recognition system and determines the system's performance to a large extent. Iris recognition produces the correct result by extracting features of the input images and matching these features with known patterns in the feature database.

IMPLEMENTATION OF ENHANCED IRIS RECOGNITION SYSTEM

Image acquirement:

Image acquirement is considered the most critical step in our project since all subsequent stages depend highly on the image quality. In order to accomplish this, we used a CCD camera. We set the resolution to 640x480, the type of the image to jpeg, and the mode to white and black for greater details. Furthermore, we took the eye pictures while trying to maintain appropriate settings such as lighting and distance to camera.

Sectionalization:

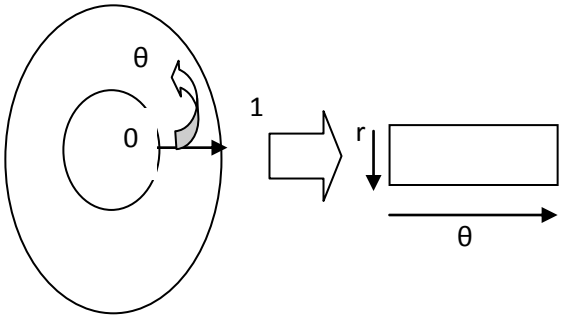
The main purpose of this process is to locate the iris on the image and isolate it from the rest of the eye image for further processing. Some other important tasks that are also performed in this iris segmentation block include image quality enhancement, noise reduction, and emphasis of the ridges of the iris. The image was filtered using Gaussian filter, which blurs the image and reduces effects due to noise. The iris inner and outer boundaries are located by finding the edge image using the Canny edge detector, then using the Hough transform to find the circles in the edge image. For every edge pixel, the points on the circles surrounding it at different radius are taken, and their weights are increased if they are edge points too, and these weights are added to the accumulator array. Thus, after all radiuses and edge pixels have been searched, the maximum from the accumulator array is used to find the center of the circle and its radius according to the equation.

$$X^2+Y^2=r^2 \text{ ---------- } (1)$$

Where *X, Y* are the center of the circle and *r* is the radius of the circle. The highest two points in the Hough space correspond to the radius and center coordinates of the circle best defined by the edge points.

Normalization:

Once the iris region is segmented, the next stage is to normalize this part, to enable generation of the "iriscode" and their comparisons. Since variations in the eye, like optical size of the iris, position of pupil in the iris, and the iris orientation change person to person, it is required to normalize the iris image so that the representation is common to all with similar dimensions. Normalization process involves unwrapping the iris and converting it into its polar equivalent.



The remapping of the iris region from the Cartesian coordinates to the normalized non-concentric polar representation is modeled as:

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta) \quad (2)$$

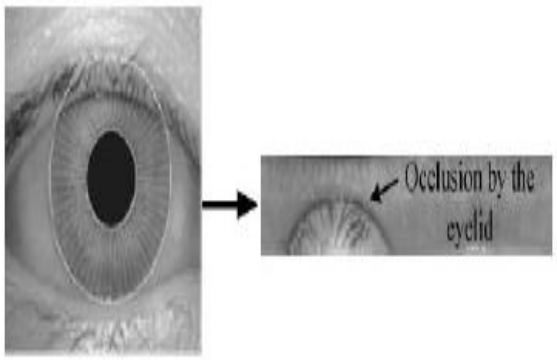
With

$$x(r,\theta) = (1-r)x_p(\theta) + rx_i(\theta) \quad (3)$$

$$y(r,\theta) = (1-r)y_p(\theta) + ry_i(\theta) \quad (4)$$

where I(x,y) is the iris region image, (x,y) are the original Cartesian coordinates, (r,) are the corresponding normalized polar coordinates, and x_p, y_p and x_i, y_i are the coordinates of the pupil and iris boundaries along the direction. In this model a number of data points are selected also each radial

line (defined as the radial resolution). The previous normalization process is demonstrated by



Since in most cases the upper and lower parts of the iris area are occluded by eyelid, it was decided to use only the left and right parts of the iris area for iris recognition. Therefore, the whole iris is $[0, 360^0]$ not transformed in the proposed system. Experiments were conducted by normalizing the iris from and $[-32, 32^0]$ and $[148, 212^0]$ ignoring both upper and lower eyelid areas as indicated in Fig. The size of the rectangular block is reduced accordingly. Left and right images each one of size 112×60 are obtained. By applying this approach, detection time of upper and lower eyelids and 64.4% cost of the polar transformation are saved. Results have shown that information in these portions of iris is subjective for iris recognition.

Feature extraction:

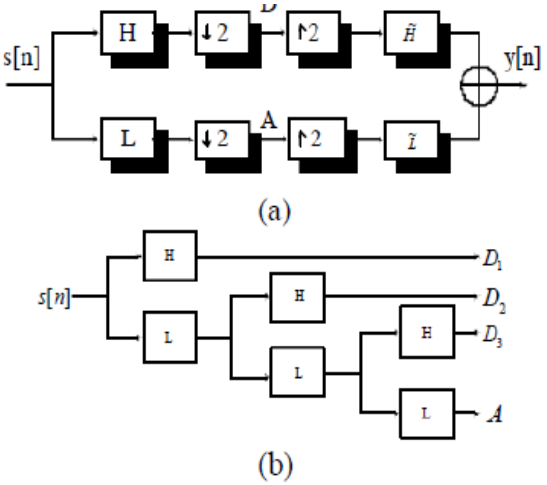
The wavelets to signal and image processing have provided a very flexible tool for engineers to apply in various fields such as speech and image processing. In an iris recognition system, the 2-D wavelet transform is only used for preprocessing.

The preprocessing helps to reduce the dimensionality of feature vector and to remove noise. Nevertheless, the computational complexity is comparatively high. Thus, the paper proposes 1- D wavelet transform as filter to reduce the dimensionality of feature vector, and it can further reduce the computational complexity. The wavelet is constructed from two-channel filter bank as shown in Fig. In wavelet decomposition of 1-D signal, a signal is put through both a low-pass filter L and a high-pass filter H and the results are both low frequency components A[n] and high frequency components D[n]. The signal y[n] is reconstructed by the construction filters *H* and *L* The wavelet filters are used to decompose signals into high and low frequency by convolution. The wavelet filters are used to decompose signals into high and low frequency by convolution.

$$D[n]=\sum_{k=-\infty}^{\infty} s[k].H[n-k] \leftrightarrow D=<s, H>$$

$$A[n]=\sum_{k=-\infty}^{\infty} s[k].L[n-k] \leftrightarrow A=<s, L>$$

In order to construct multi-channel filter, we can cascade channel filter banks. Fig. represents a 3-level symmetric octave structure filter bank.



(a) Two-channels filter bank
(b) 3-level octave band filter bank

Identification:

The last module of an iris recognition system is used for matching two iris templates. Its purpose is to measure how similar or different the templates are and to decide whether they belong to the same individual or not. An appropriate match metric can be based on direct point-wise comparisons between the phase codes [8]. The test of matching is implemented by the XOR operator that is applied to the encoded feature vector of any two iris patterns. The XOR operator detects disagreement between any corresponding pair of bits. The system quantifies this matter by computing the percentage of mismatched bits between a pair of iris representations, i.e., the normalized Hamming distance. Let *X* and *Y* be two iris templates to be compared and *N* be the total number of bits so, *HD* is equal to the number of disagreed bits divided by *N* as shown in equation 5.

$$HD = \frac{1}{N} \sum_{j=1}^{N} X_j$$

In order to avoid rotation inconsistencies which occur due to head tilts, the iris template is shifted right and left by 8 bits. It may be easily shown that scrolling the template in polar coordinates is equivalent to iris rotation in Cartesian coordinates. The system performs matching of two templates several times while shifting one of them to four different locations. The smallest HD value amongst all these values is selected, which gives the matching decisions.

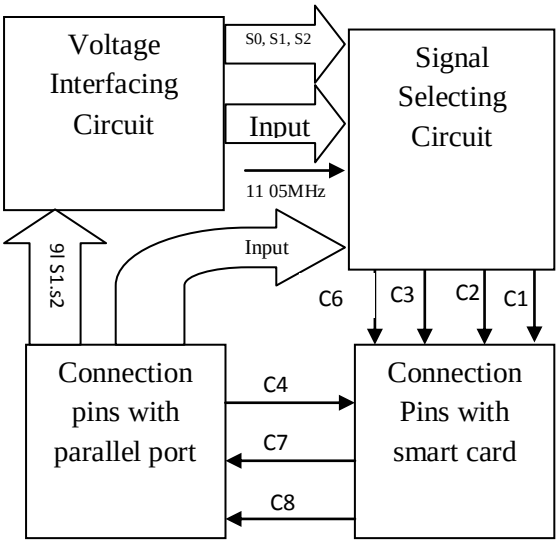
BIOMETRIC SMART CARD

Biometric technologies, when used with a well designed ID system, can provide the means to ensure that an individual presenting a secure ID Credential has the absolute right to use that credential. Smart cards have the unique ability to store large amounts of biometric and other data, carry out their own on-card functions, and interact intelligently with a smart card reader. Secure ID systems that require the highest degree of security and privacy are increasingly implementing both smart card and biometric technology. According to the definition smart card is “a device that includes an embedded integrated circuit that can be either a secure microcontroller or intelligent equipment with internal memory” [10]. A well known type of smart cards is the Fun Card. The Fun card belongs to microprocessor-contact smart

card. It consists of the AT90S8515 microcontroller which is a low-power CMOS 8-bit microcontroller and the AT24C64 EEPROM which provides 65,536 bits of serial electrically erasable and programmable read only memory [11].

Smart Card Programmer:

The smart card programmer has been designed to enable read/write from/to the smart card. The programmer is connected to the PC using the parallel port, due to its higher speed compared with serial port and the ability to generate multiple signals at the same time. The block diagram shown in Fig. consists of four parts which are: signal selection circuit, voltage interfacing circuit, connection pins to the parallel port, and connection pins to the smart card. Where C1-C8 are the pins of the smart card and S0-S2 are the selecting signals.



The block diagram of designed programmer.

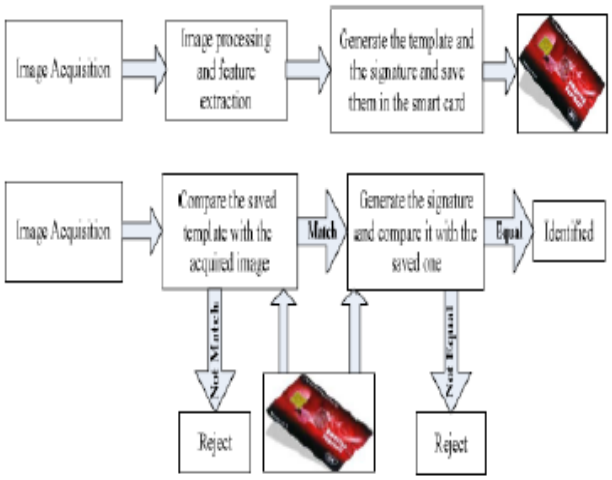
Table 1 shows the function of each pin in the used smart card.

Table 1: Description of each pin used in smart card

Pin No.	Name	Function	Direction
C1	Vcc	Power supply 5 VDC	In
C2	Reset	CPU Reset line	In
C3	XTAL	Main clock up to 11MHz	In
C4	MOSI	SPI master input	In
C5	Vss	Power Ground	In
C6	Nc	Not Connected	--
C7	MISO	SPI Master output	Out
C8	SCK	SPI serial clock	In

Integrating Iris Recognition with Smart Card:

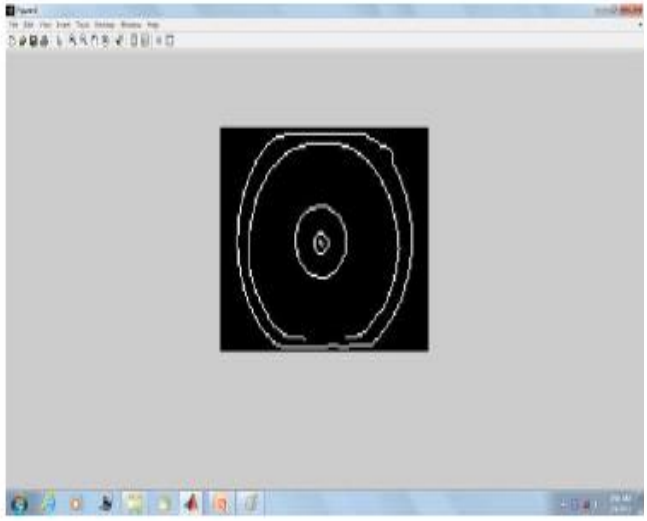
After extracting data from iris image, it is saved in the smart card's flash memory using the smart card programmer. Extracted iris features stored in smart card are compared against the acquired data from the camera or the database to confirm that a person is authenticated or not. In order to protect the data against manipulation, a signature of the data has been generated using the MD5 hash function, which produces 18 bytes signature, and then saved in the smart card. Hence, in the identification process, the system generates the biometric template and its signature from the acquired data and compare them against the smart card contents. In case of finding any difference between the generated and the saved template or signature, the identification is rejected. Fig. shows the block Diagram of the designed system.



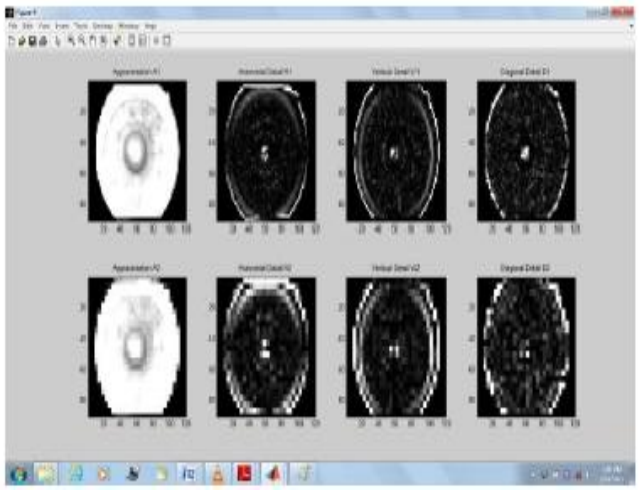
The block diagram of the designed system.

Experimental Result Using MATLAB:

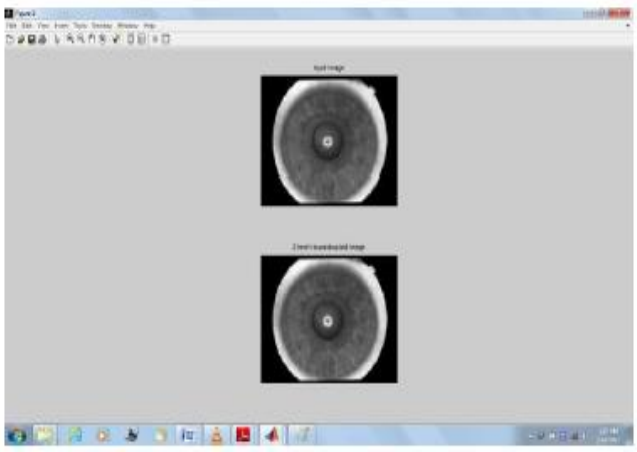
The result is reported by Fig. 8 (a), (b), and (c). The proposed technique has found the edges from the images which are very evident and clear by the visualization.



Detected edge in an image



2D-wavelet transformed image



2D-wavelet deconstructed image

CONCLUSION

Iris images are obtained from the Chinese Academy of Sciences Institute of Automation CASIA Ver. 1 database [11]. The database consists of 756 iris images from 108 classes enhance the performance of iris recognition system by using the canny edge detection and statistical features for iris recognition. In which we tested the comparison of two iris patterns by using hamming distance. We have successfully developed this new Iris Recognition system capable of comparing two iris images. This identification system is quite simple requiring few components and effective enough to be integrated within security systems that require an identity check.

REFERENCES

[1]. G. Bella, S. Bistarelli, and F. Martinelli, "Biometrics to Enhance Smartcard Security". Lecture Notes in Computer Science, vol. 3364, 2005.

[2]. M. Bond, and P. Zielinski, "Decimalization table attacks for pin cracking". Technical Report UCAM-CL-TR-560, University of Cambridge, Computer Laboratory, 2003.

[3]. L. Bechelli, S. Bistarelli, and A. Vaccarelli, "Biometrics authentication with smartcard". Technical Report, CNR, Istituto di Informatica e Telematica, Pisa, 2002.

[4]. H. Proença, and A. Alexandre, "Towards non cooperative iris recognition: A classification approach using multiple signatures". IEEE Trans. vol. 29, pp. 607-612, 2007.

[5]. S.K. Pedersen, "Circular Hough Transform". Aalborg University, Vision Graphics and Interactive Systems, 2007.

[6]. M. Nabti, and A. Bouridane, "An effective and fast iris recognition system based on a combined multiscale feature extraction technique". Pattern Recognition, vol. 41, pp. 868–879, 2008.

[7]. FU Zhenghua, LI Yongjun, Tian Mi (2007). "The embedded monitoring system based ARM". JOURNAL OF 7INSTRUMENT TECHNOLOGY, Vol. 07, No. Ipp. 01-2.

[8]. Jun Zhou, Guangda Sua, Chun hongJiang. A face and fingerprint identity authentication system based on multi-route detection. Neuro computing 70 (2007)922-931.

[9]. Yuliang He, Jie Tian, Xiping Luo, Tanghui Zhang. Image enhancement and minutiae matching in fingerprint verification. Pattern Recognition Letters 24 (2003)1349-1360.

[10]. Wei Wang, Jianwei Li, Feifei Huang, Hailiang Feng. Design and implementation of Log-Gabor filter in fingerprint image enhancement. Pattern Recognition Letters 29 (2008)301-308.

[11]. Center of Biometric and Security Research, Iris Database. CASIA VI. Available Online: http://cbsr.ia.ac.cn/english/IrisDatabase.asp

Short Bio Data for the Author

Mr. C. Raghavendra received his Master Degree of Computer Science and Engineering from Bharath University, Chennai. He has 2 years of teaching experience and his specialization are Image processing, Computer Networks, Network Security, Design Analysis and Algorithms.

Dr.S.Sivasubramanain, M.Tech(CSE)., Ph.D(CSE). as an professor from Department of Information Technology Dhanalakshmi College Of Engineering Approved by AICTE and Affiliated to Anna University Chennai, Tamil Nadu. an NBA Accredited and ISO 9001:2008 Certified Institution. He has more than 11 years of teaching and research experience and his areas of specialization are mobile computing, Database Management System, Computer Networks, Networks Security and Data Mining.

Dr.A.M.Sameeulla, M.sc(Engg)., Ph.D(CSE). as an professor from Department of Computer science and Engineering, Approved by AICTE and Affiliated to Anna University Chennai Tamil Nadu an NBA Accredited and ISO 9001:2008 Certified Institution. He has more than 38 years of teaching and research experience and his areas of specialization are Parallel Programming and Computer Networks