Volume 2, No. 7, July 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESERCH PAPER
Available Online at www.jgrcs.info

PATTERN RECOGNIZATION USING NEURAL NETWORK OF HAND BIOMETRICS

Amit Taneja*[1] and Sonika [2]
[1]Computer Engineering Section, Yadavindra College of Engineering, Talwandi Sabo
amit_t19@yahoo.com
[2]Department of information Technology ,B.H.S.B.I.E.T, Lehragaga
sonika_bhandari@rediffmail.com

Abstract-- In today's world, biometric identifications are gaining more and more importance. A biometric system provides more reliable and efficient means of identity verification. The physical dimensions of a human hand known as hand or palm geometry, contains information that is capable of authenticating the identity of an individual. The hand geometry based identity verification system is being widely used in various applications like access control, time and attendance. The goal of a biometric verification system consists in deciding whether two characteristics belong to the same person or not. It explores the features of a human hand, extracted from a color photograph which is taken when the user is asked to place his/her hand on a platform especially designed for this task.

Keywords-- Biometric verification, Hand geometry, Landmarks, Palmprint recognition, Neural networks.

INTRODUCTION

Biometric is the most secure and convenient authentication tool. It cannot be borrowed, stolen, or forgotten and forging one is practically impossible. Biometrics measure individual's unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometrics includes fingerprints, hand or palm geometry, retina, iris, and facial characteristics. Behavioral characters characteristics include signature, voice, keystroke pattern, and gait. Of this class of biometrics, technologies for signature and voice are the most developed. Biometrics is the science of using human measurements to identify people. Today, an individual's identity can be verified using physical means by scanning his fingers, hands, eyes, or face. He can also be verified by behavioral means. His gait, vocal pitch, signature, and typing speed can be used to identify him.[4].

Biometric technology offers the promise of an easy, secure method to make highly accurate verifications of individuals. Not only does this technology make our lives easier by eliminating the need to carry badges and other identification, but it prevents the use of forged tickets, badges, or passports. These verifications have broad applicability, and people are already being verified by biometrics in airports, office buildings, manufacturing centers, hospitals, and even amusement parks. A biometric scan can provide security access to protected areas, serve as a day pass at an attraction, punch an employee in at the start of the work day, or allow an executive access to his laptop computer.

Biometric is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification and keystroke dynamics are examples of behavioral characteristics.

Biometric authentication requires comparing a registered or enrolled biometric sample against a newly captured biometric sample for example, a fingerprint captured during a login. During enrollment a sample of the biometric trait is captured, processed by a computer, and stored for later comparison.[1].

Biometric recognition can be used in Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. This is sometimes called "one-to-many" matching. A system can also be used in Verification mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user.

Security Parameters of Biometrics

Unique: The various biometrics systems have been developed around unique characteristics of individuals. The probability of 2 people sharing the same biometric data is virtually nil.

Cannot be Shared: Because a biometric property is an intrinsic property of an individual, it is extremely difficult to duplicate or share (you cannot give a copy of your face or your hand to someone!).

Cannot be Copied: Biometric characteristics are nearly impossible to forge or spoof, especially with new technologies ensuring that the biometric being identified is from a live person.

Cannot be Lost: A biometric property of an individual can be lost only in case of serious accident.

Working Principle of Biometric Technologies

Biometric technologies capitalize upon unique, permanent, and scannable human characteristics. A unique characteristic is one that no other person shares. This characteristic should also remain the same over time, and be reliably collectable using a sensor. As much as possible, biometric technologies focus upon these types of human traits.

All biometric devices take a number of measurements from an individual then digitally process the result of these measurements and save this representation of the individual's traits into a template. Templates are then stored in a database associated with the device or in a smartcard given to the individual. This is called enrollment.

At their most basic level, biometric technologies are pattern recognition systems that use either image acquisition devices, such as scanners or cameras in the case of fingerprint or iris recognition technologies, or sound or movement acquisition devices, such as microphones or platens in the case of voice recognition or signature recognition technologies, to collect the biometric patterns or characteristics.[5]

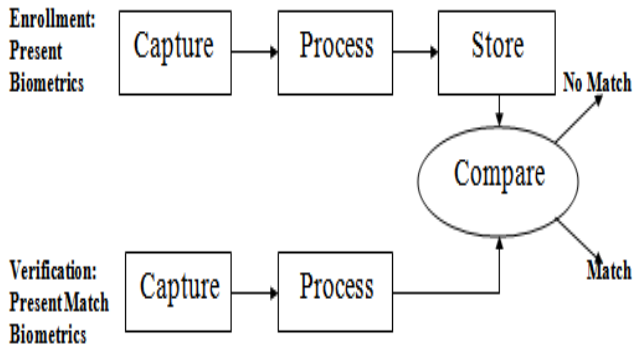

Figure 1(a): Generic biometric processes

Selecting a Biometric Technology

There are a number of biometric technologies available at the moment. It is very critical to pick up the one which meets the user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters. Here comes some of the key points to be taken into account before selecting one.

Ease of use - some biometric devices are difficult to handle unless there is proper training.

Error incidence - Time and environmental conditions may affect the accuracy of biometric data. For instance, biometrics may change as an individual becomes old. Environmental conditions may either alter the biometric directly (if a finger is cut and scarred) or interfere with the data collection (background noise when using a voice biometric).

Accuracy - Vendors often use two different methods to rate biometric accuracy: false-acceptance rate (FAR) or false-rejection rate (FRR). Both methods focus on the system's ability to allow limited entry to authorized users. However, these measures can vary significantly depending on how one adjust the sensitivity of the mechanism that matches the biometric. There may be instances where FAR decreases and FRR increases. Thus we have to be careful to understand how the biometrics vendors arrive at quoted values of FAR and FRR. Because FAR and FRR are interdependent, we can draw a plot, which can facilitate to determine the crossover error rate (CER). The lower the CER, the more accurate the system

Performance Measures

The performance of a biometric system is measured in certain standard terms.

These are main three types of standard terms given below-

False Acceptance Rate: FAR is the ratio of the number of unauthorized users accepted by the biometric system to the total of identification attempts to be made. This is also known as type 2 error, False Acceptance Rate is when an imposter is accepted as a legitimate user, This happens when the system find that the biometric data is similar to the template of a legitimate user. FAR is calculated by FAR (λ) = Number of False Attempts / Total Number of Attempts

Where (λ) = Security Level.

False Rejection Rate: FRR is the ratio of the number of number of authorized users rejected by the biometric system to the total number of attempts made. False Rejection Rate known as type 1 error, when a legitimate user is rejected because the system is not found that the current biometric data of the user similar to the biometric data in the templates that are stored in the database. Now since there is no zero error in a system that is in the real world, we calculate the FRR using a simple math equation:

FAR(λ) = Number of False Rejections / Total Number of Attempts

Equal Error Rate: Equal error rate is a point where FRR and FAR are same. The ERR is an indicator on how accurate the device is, the lower the ERR is the better the system.

Now if we have a score of the FAR & FRR we can create a graph that indicates the depends of the FAR & FRR on the threshold value. The following is graph is an example:

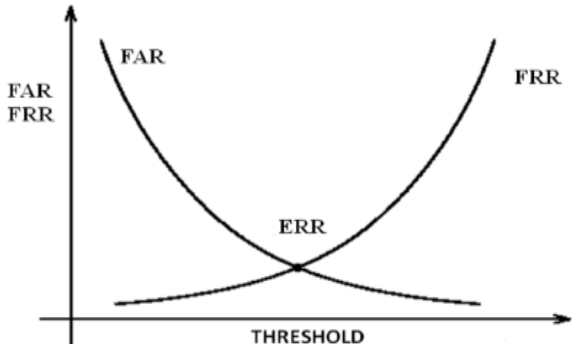

Figure 1(b): Equal Error Rate

BIOMETRIC TECHNIQUES

Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric characteristics can be divided in two main classes Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, which has largely replaced retina, and odour/scent.

Behavioral are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term behavior metrics for this class of biometrics

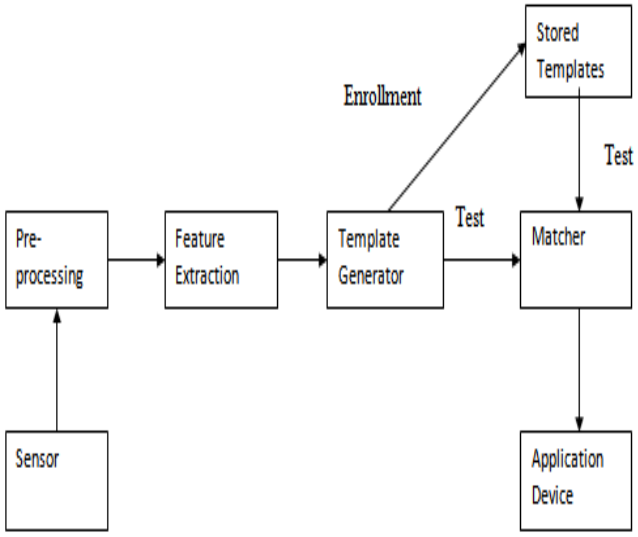

Figure 2: Biometric Technique

HAND GEOMETRY

A variety of measurements of the human hand can be used as biometric characteristics. These include hand shape, the lengths and widths of the fingers, and the overall size of the hand. Biometric devices based on hand geometry have been installed at many locations around the world. The hand-geometry technique is simple, relatively easy to use, and inexpensive.

Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in various places around the world. The technique is very simple relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems.

The hand images can be obtained by using a simple setup including a web cam. However, other biometric traits require a specialized, high cost scanner to acquire the data. The user acceptability for hand geometry based biometrics is very high as it does not extract detail features of the individual. Thus, for applications where the biometric features are needed to be distinctive enough for verification, hand geometry can be used.[13]

Hand Geometry Biometric System Module

A biometric system consisting of five important modules, first module is image acquisition which reads image, second module is image preprocessing which include Conversion to Gray scale, Applying Thresholding, De-Noise, Edge Detection, Morphology Optimal dilation and erosion Third module is feature extraction, Fourth is matching, and Fifth is decision. Firstly image of hand is captured through a digital camera/scanner then it is fed to

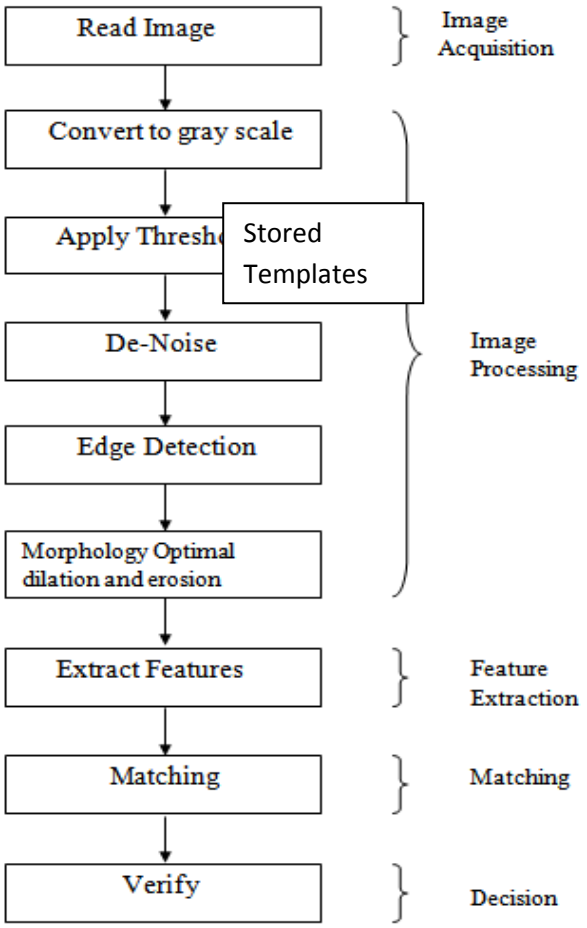

Figure 3(a): Hand Geometry Biometric System Module

The next module i.e. image preprocessing module. The role of the preprocessing module is to clean up the noise because the input image having some noise due to dust on the palm, atmospheric conditions.

The processing module is used to prepare the image for feature extraction. The feature extraction module is very important module in a hand geometric system. The function of this module is to extract and store features from the input image. The output of the feature extraction module is the measure of features like finger length, finger width, palm width etc. The next module of this system is matching. Here the features extracted in the previous section are matched up with the features of that individual previously stored in the database. Therefore, matching is a straight one to one comparison between scanned and stored data. The last module of the hand geometrics biometric system is decision module. This module gives a 'yes' or 'no' response to the user and to a high degree of accuracy.[12]

Image Acquisition

The first stage of any vision system is the image acquisition stage. The image acquisition involves capturing and storing digital images from vision sensors like color digital cameras, monochrome and color CCD cameras, video cameras, scanners etc. The image acquisition system comprises of a light source, a digital camera/scanner. The input image is a color/grayscale image of the hand palm. In this proposed system images are acquiesced through a digital camera. It is necessary that the fingers are separated from each other. However it is not required to stretch the fingers too far apart as possible. The hand should be placed in a relaxed state

with fingers separated from each other. Since features such as length and width which are dependent on the image size and resolution are being used, it is critical that to have uniform size of images. There are various format stored for the images such as .jpeg, .tiff, .png, .gif and bmp. The captured images are stored in one of the following formats on the computer for possible image processing. After the image has been obtained, various methods of processing can be applied to the image to perform the many different vision tasks required today.

Figure 3(b): Image acquisition

Image Preprocessing

The next stage is image preprocessing module. Image preprocessing relates to the preparation of an image which includes Conversion to Gray scale, Applying Thresholding, De-Noise, Edge Detection, Morphology Optimal Erosion, Dilation for later analysis and use. Images captured by a camera or a similar technique are not necessarily in a form that can be used by image analysis routines. Some may need improvement to reduce noise; other may need to simplified, enhanced, altered, segmented, filtered, etc. The role of the preprocessing module is to prepare the image for feature extraction. The first step in the preprocessing block is to transform the color image into a gray scale image and this result to noisy gray scale image. In the next step, filtering is used in order to cancel the presented noise. Then, edge detection algorithm is applied for obtaining edge of the noiseless gray scale image. Image preprocessing module is consist of following operations[12]

Gray Scale Image: In this proposed system hand image is captured through digital camera so the original image is colored image. For digital image processing it is necessary first colored hand image convert in to grayscale image. Basically grayscale is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest. Now color hand image is converted in to gray scale image with noise because there is some noise present in the input colored image due to dust and atmospheric conditions. This noise removal is therefore essential for the system.

Noise Removal: The next step in image preprocessing is noise removal. It is necessary to remove the noise from the image because it may produce difference between the actual palm and captured image. This causes the variation in data base feature and measured feature and also affected the accuracy of the system. Another reason of noise removal is that edge detection is difficult in noisy images, since both the noise and the edges contain high frequency content Basically the noise produced in the image is due to device using for capturing image, atmosphere condition or surrounding. There are many methods to remove the noise in Matlab. In this proposed system the noise is removed by wiener2 filter. So before extracting features from the image, it is very important to remove the noise from the image. Attempts to reduce the noise result in blurred and distorted edges. Operators used on noisy images are typically larger in scope, so they can average enough data to discount localized noisy pixels. This results in less accurate localization of the detected edges.[13]

Edge Detection: In order to extract geometric features of the palmprint it is required that the image contains only edges. Edge detection is the process of localizing pixel intensity transitions. The edge detection has been used by object recognition, target tracking, segmentation, and etc. Let‘s consider the boundary detection under image enhancement because the goal is to emphasize features of interest i.e. boundaries and attenuate everything else.

Edges play quite an important role in many applications of image processing, in particular for machine vision systems that analyze scenes of man-made objects under controlled illumination conditions. Detecting edges of an image represents significantly reduction the amount of data and filters out useless information, while preserving the important structural properties in an image.

Feature Extraction

The next module of hand geometry biometrics is feature extraction. In pattern recognition and in image processing, feature extraction is a special form of dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be notoriously redundant means much data, but not much information then the input data will be transformed into a reduced representation set of features also named features vector. Transforming the input data into the set of features is called feature extraction. If the features extracted are carefully chosen it is expected that the features set will extract the relevant information from the input data in order to perform the desired task using this reduced representation instead of the full size input.

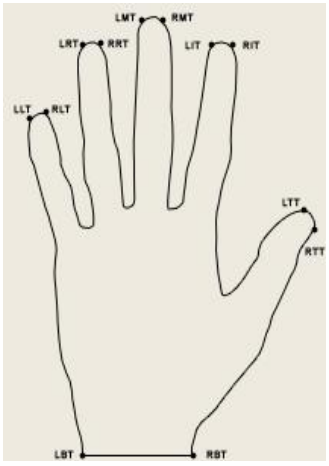

Figure 3(c): Features extracted from the input image

The hand geometry-based authentication system relies on geometric invariants of a human hand. Typical features include length and width of the fingers, aspect ratio of the palm or fingers, thickness of the hand, etc. The first feature that can be extracting is the length of a finger. The second

major feature is the width of the finger. One or more measurements can be taken for the width at varying points along the finger. The length of the lines on the finger can also be used as the measure of finger width. Since the fingers may not have uniform width usually two or more measurements are taken for each finger along different points.

Matching

The last module of the biometric system is matching. The feature matching determines the degree of similarity between stored feature vector and claimed feature vector. Here the features extracted in the previous section are matched up with the features of that individual previously stored in the database. The matching step actually quantifies the level of similarity between two hand templates. Besides that, most hand recognition systems also incorporate the optional step of updating the reference template in the enrollment database. Over the years, hand recognition is said to be more suitable for verification purpose only, as the hand features are not unique for everyone. The possibility for having two people with similar hand features increases with large Population. Distance functions are used to decide whether the claimer is the claimed person or not. In this proposed system absolute distance function is used for matching the feature vector.

Decision

After calculating the distance, the system compares the result with a predefined threshold and classifies the claimer. The system accepts the claimer if and only if the calculated distance is lower than the threshold, and it rejects the claimer if and only if the calculated distance is higher than the threshold.

PROBLEM FORMULATION & PROPOSED SOLUTION

Problem Formulation

With the advancement of automation and the development of new technological systems personal identification is necessary in our daily lives. Biometrics technology allows determination and verification of one's identity through physical characteristics. Biometrics is a more foolproof form of authentication than typing passwords or even using smart cards, which can be stolen. Biometric systems replace conventional identification techniques since these are more convenient and reliable. Hand geometry based biometric system plays a very important role in personal verification applications. Hand geometry biometric systems can be used in low to medium security applications. If this system combined with fingerprints and palmprint in a multi modal system it can prove very useful in high security applications. The advantage of combining these features lies in the fact that while taking the data for hand geometry, the data for fingerprints and palmprint can be collected simultaneously. Most of the present available hand geometry system always uses pegs to fix the placement of the hand. The main weaknesses of using pegs are that pegs deform the shape of the hand and users might place their hands incorrectly. These problems can certainly reduce the performance of the biometric system. Another problem with these pegs is that it is not possible collect the data for hand geometry, fingerprints and palmprint, simultaneously in a multimode biometric system. The purpose of this research is to design a biometric system based on hand geometry without pegs. Therefore, users can place their hands freely on the system platform. These types of biometric systems are not complex and yields good performance.[10]

Proposed Solution

The proposed hand geometry biometric system provides a new approach to extract the hand geometry features. Data is read and processed independently of the position of the user hand. In this system, the selected features are not varying with variation of hand position. The main goal of this project work is to implement a system which can be able to acquire the images freely without any restriction by allowing the user to put his/her hand virtually in any position.

The proposed system extracts the left and right tip of each finger and also takes left and right tip point of thumb. Also the palm width and two other distances between left tip point of little finger and bottom left point of palm and between right tip point of thumb and bottom right point of palm are measured. The most important geometric part of the palm for feature extraction is the fingers. For each finger and thumb two points, one is left top tip and second is right top tip are taken which makes it a total of 10 features for the four fingers and thumb. Including palm width and two other distances and two ratios brings the number of total features to 17. All the landmark points on the right hand palm are defined below and shown in fig .5.1

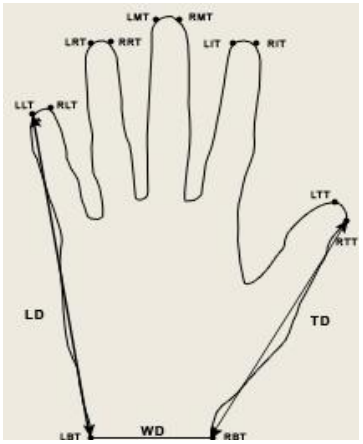

Figure 4: Define all landmark point and all features

WD- Distance between two bottom points of palm LD- Distance between left tip point of little figure and bottom left point of palm TD- Distance between right tip point of thumb and bottom right point of palm

R_1- Ratio R_1

R_2- Ratio R_2

In this proposed system 21special features extracted from the palm. The definition of these features are given below

(i) The "WD" is obtained by measuring the distances from the bottom left point of palm to the Bottom right point of palm as shown in fig.5.1. .

(ii) The "LD" is obtained by measuring distances from left tip point of little finger to bottom left point of palm as shown in fig 5.1.

(iii) The "TD" is obtained by measuring distances from right tip point of thumb to bottom right point of palm as shown in fig. 5.1
(iv) Ratio R_1 is calculated by dividing LD / TD.
(v) Ratio R_2 is calculated by dividing TD / WD.

RESULTS AND DISCUSSION

In any pattern Recognization application there are many variables which define the pattern which takes the definitive or deterministic lattice, this is following a certain mathematically derivable co-relation between and among these variable defining the pattern. The first step normally involves identify highly significant variables which defines the pattern. In our case the various bio-geometric measurements were selected as the parameters which defines the pattern of recognition, these co-relation between and among themselves clearly reflects a unique pattern to each subject in question for authorization and verification to a hypothesis of detection and analysis for identifying for a genuine or imposter entering our system. Here are the following parameters which defines our mathematical model for doing discriminant analysis from authorized and unauthorized person.

X_1 = TopFigTipX
X_2 = TopFigTipY
X_3 = ThumTipX
X_4 = ThumTipY
X_5 = LittleFigTipX
X_6 = LittleFigTipY
X_7 = RingLeftFigTipX
X_8 = RingLeftFigTipY
X_9 = RingRightFigTipX
X_{10} = RingRightFigTipY
X_{11} = IndexRightFigTipX
X_{12} = IndexRightFigTipY
X_{13} = Ratio R_1
X_{14} = Ratio R_2

In general, the relationship between and among these pattern defining parameters or observation may be anything but unique to a subject. Once we have established the fact that these bio-metric observations are highly co-related to each other and to identification process and its value is equal to 1 and to proceed further regression analysis was done to know the correct nature of the co-relation stated above. The bio-variant grouped data analysis helped us to identify an un authorized or un authorized person (subject).

Mean Squared Error

It can also be further independent from above graphs that the mean squared error is also reducing in each stage, especially after the back propagation algorithm training. It must be noted that if the standard error of estimate is closed to zero that means that the regression model have been comfortably been able to identify true nature of fitting of the pattern parameters(dependent or independent variables).

Confusion Matrix

A research basically is about continuous valued function for example a classification model build to identify safe or risky and at the same time to predict the potential of customize expenses. Similarly in our case we have done data classification in two steps:

- First step includes the training data sets or training samples
- Second step includes the machine learning using back propagation learning.

In our case the predictive accuracy of person being identified as authorized or un authorized depends upon the accuracy of sample size taken for training. In our case we have taken 5 images per subject and observed 100 subjects. The model we have build is highly scalable and interpretability can be understood in terms of its confusion matrix graph as shown above. Our system is highly tolerant to the noisy data and has ability to classify data that is not trained, during the learning process the network learns by adjusting the various weights so that it is able to predict correct class labels of input sample, here it is how it is learning using back propagation algorithm.

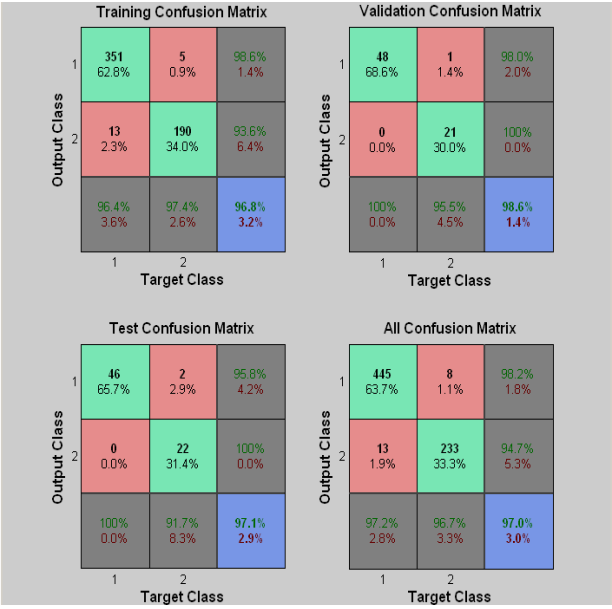

Figure: 5(a): Confusion Matrix

Algorithm: Backpropagation

Neural network learning for classification, using the Backpropagation algorithm.
Input: The training samples, samples; the learning rate, l; a multilayer feed-forward network, network.
Output: A neural network trained to classify the samples.
Method:

1. Initialize all weights and biases in network;
2. **while** terminating condition is not satisfied {
3. **for** each training sample X in sample {
4. // Propagate the input forward:
5. **for** each hidden or output layer unit j {
6. $I_j = \sum_i w_{ij}O_i + \Theta_j$; //compute the set input of unit j with respect to the previous layer, i
7. $O_j = 1/ 1 + e^{-1}$; } // compute the output of each unit j
8. // Backpropagate the errors:
9. **for** each unit j in the output layer
10. $Err_j = O_j(1 – O_j)(T_j – O_j)$;// compute the error
11. **for** each unit j in the hidden layers, from the last to the first hidden layer
12. $Err_j = O_j(1 – O_j)$ // compute the error with respect to the next higher layer, k
13. **for** each weight w_{ij} in network {
14. $\Delta w_{ij} = (l)Err_jO_i$; // weight increment

15. $w_{ij} = w_{ij} + \Delta w_{ij}$; } // weight update
16. **for** each bias Θ_j in network {
17. $\Delta\Theta_j = (l)Err_j$;// bias increment
18. $\Theta_j = \Theta_j + \Delta\Theta_j$; }// bias update
19. } }

It can be seen from the confusion matrix that the overall classification accuracy finally increases towards a value of 100% as the training is completed. The confusion matrix basically gives us the view after considering the Receiving Operating Characteristic (ROC).

In the above diagram we can see that true positive and false positive rate have been calculated t each stage of training, validation and testing. The value of all these graphs gas been calculated based on formula used to calculate threshold as follow.

This threshold basically classifies people from being authorized or unauthorized.

Performance

As it can be seen from above graph the intersection point shown in the graph signifies point where the data set passes through each phase is optimally performing with respect to MSE. The optimal performance point is (8, 10^{-2})

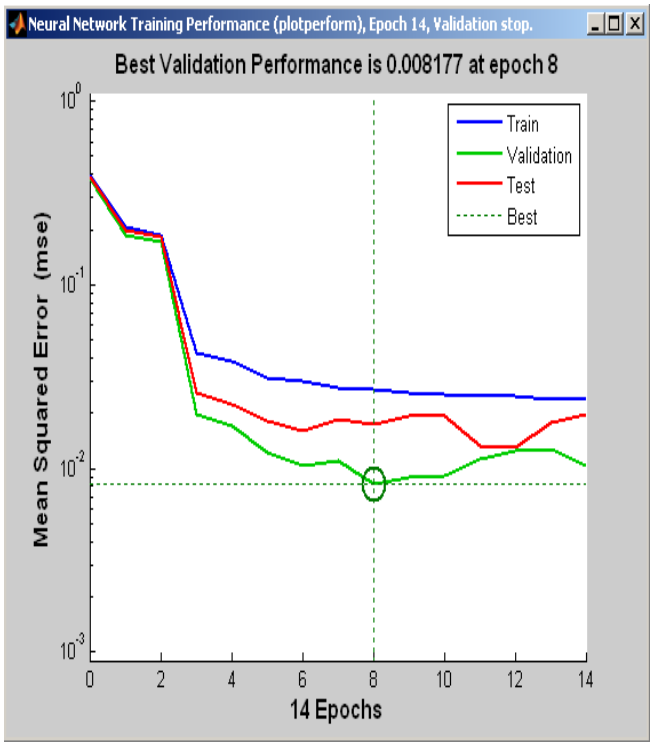

Figure 5(b): Neural network training performance

All ROC

Fig 7.6 is the ROC curve showing the All performance of Hand Bio metric system operated as unimodal. On the ROC curve, the higher the line is drawn, the grater the GAR is .97 and therefore the more the accurate is the system. There are different FAR intervals, each of them have a corresponding GAR value. has the highest value of 82% GAR at 18% FAR. The receiver operating characteristics (ROC) curve are used extensively used for performance evaluation in biometrics systems therefore, this analysis is conducted at each stage.

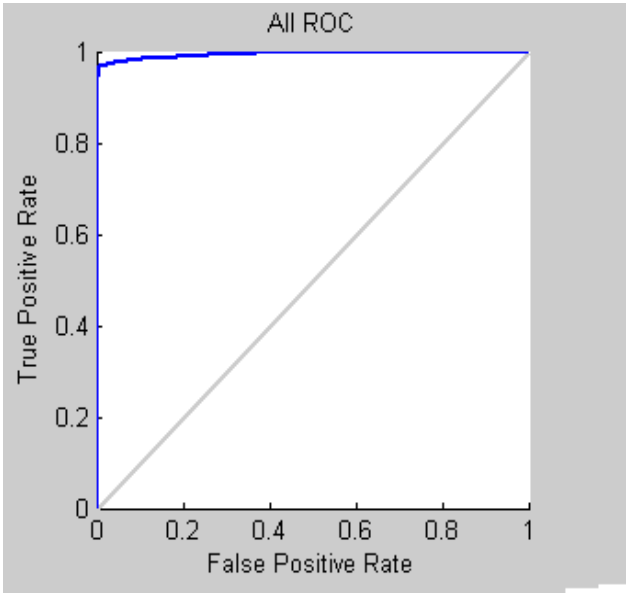

Figure 5(c): All ROC

CONCLUSION

A peg-free hand-geometry verification system has been developed in this thesis work which is independent of orientation and placement of the hand. The system is experimented with a database consisting of 500 images collected over time from 100 users. 5 sample images from each user were used for verification purpose. The verification system extracts the feature vector from the image and stores the template for later verification. FRR is obtained by comparing the two feature vectors of the same hand and FAR is obtained by comparing the feature vectors of two different hands.

The system shows effectiveness of results with accuracy around 89%. and the FAR to be around 0.18.

This special project would detect a user is a member of a system or not. If he/she is a valid user of the system, then he/she is identified and the output is 'Yes'. If the user could not be identified by the system, it output is No'. Implementation of the program would result in a much secure and accurate system.

SCOPE OF FURTHER WORK

These days support vector machines have gaining lot of importance for doing classification and prediction in the field of machine learning, although Back Propagation Algorithm is highly successful algorithm till date for machine learning and having very wide application in bioinformatics. The Back Propagation Algorithm has been also be used by physiologist and neuro-biologist, but in recent development support vector machine has been found place in bio informatics fertinity. For future scope some more bio-metric matrices with support vector machines

REFERENCES

[1] Raymond Veldhuis, Wim Booij, Asker Bazen and Anne Hendrikse, "A Comparison of Hand-Geometry Recognition Methods Based on Low- and High-Level Features", University of Twente, Netherlands, pp 326-330, 2002.

[2] Guangming Lu, Zhang David, and Kuanquan Wang, "Palmprint Recognition Using Eigen Palms Features", Pattern Recognition. Letters, pp 143–146, 2003

[3] Kresimir Delac, Mislav Grgic, "A Survey of Biometric Recognition Methods", 46th International Symposium Electronics in Marine, ELMAR- 2004 Zadar, Croatia, pp 16-18, June 2004.

[4] Jain, Ross and Prabhakar. "An Introduction to Biometric Recognition", IEEE Transaction on Circuits and Systems for Video Technology, January 2004.

[5] 5 Sekhar Chandra C., Naidu Prakash and Shrivastava Sangeeta, "Biometric Verification Using Contour-Based Hand Geometry and Palmprint Texture", Proc. of the 18th International Conference on Pattern Recognition, pp 1208-1214, 2006.

[6] Kumar A., Wong M., Shen H., and Jain A. K., "Personal Authentication Using Hand Images", Pattern Recognition. Letters, Vol. 27, no. 13, pp. 1478– 1486, October 2006.

[7] Yoruk E., Konukoglu, Sankur B., and Darbon, "Shape-Based Hand Recognition", IEEE Transaction on Image Processing, Vol. 15(7), pp. 1803- 1815, 2006.

[8] Morales Aythami, Ferrer A. Miguel, Francisco Díaz, Jesús B. Alonso and Carlos M. Travieso "Contact-free Hand Biometric System for Real Environments" Technological Centre for Innovation in Communications University of Las Palmas de Gran Canaria Campus de Tafira, 35017, Las Palmas, Spain, 2008.

[9] Niennattrakul Vit and Ratanamahatana Chotirat, "Making Hand Geometry Verification System More Accurate Using Time Series Representation with R-K Band Learning" Department of Computer Engineering, Chulalongkor University Phayathai Rd., Pathumwan, Bangkok 10330 Thailand, pp 120-128, 2008.

[10] Aghili Bahareh and Sadjedi Hamed "Personal Authentication Using Hand Geometry" Department of Electrical Engineering. Shahed University Tehran, Iran IEEE Transaction, 2009.

[11] Kanhangad Vivek and Zhang David, "Combining 2D and 3D Hand Geometry Features for Biometric Verification", Department of computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong IEEE Transaction pp 39-44, 2009..

[12] Casanova Guerra, Sierra Santos, "Silhouette-based Hand Recognition on Mobile Devices", IEEE Transaction pp 160-166, 2009.

[13] Chandra Bhan Pal and Amrit Kumar Agrawal, "Hand Geometry Verification System: A Review", Department of Computer Science & Engineering, Jaypee University of Information Technology, Wakanaghat, Solan, (H.P), India.

