Biometric Parameters & Palm Print Recognition

G. Seshikala
Dept. of ECE, AIT
Bangalore

Umakanth Kulkarni
Prof & HOD CSE, SDMCET
Dharwad

M.N. Giriprasad
Prof Dept. of ECE, JNTUA
Ananthapur

ABSTRACT
A successful biometric system depends on the accuracy with which it works. The degree of accuracy is measured with biometric parameters. This paper addresses the various parameters used in the analysis and measurement of a Biometric system. This paper also presents experimental results of a palm biometric with a POLY U database. The performance is measured with a variable threshold.

General Terms
Biometrics, Biometric parameters, Feature extraction

Keywords
Biometrics, FRR, FAR, EER, GAR,ROC, DET, CMC, Palm recognition

1. INTRODUCTION
Biometric system is a pattern recognition system which uses physiological traits (i.e. face, palm, and iris) or behavioral traits (i.e. speech, signature) for verification and identification. The biometric approach identifies an individual or verifies the claimed identity by extracting the feature of the biometric trait which is given as an input and matching it with the data base available. A Biometric system has four stages of processing. In the**sensor stage**, a biometric image is captured and enrolled as an input to the system which is used for verification or identification. In the **featureextraction stage**, the feature of the enrolleddata is extracted and stored as a feature set and is further processed for verification or identification. In the**Matching stage,**thefeatures extracted are matchedwith the stored features set in the database and the degree of similarity is measured as a matching score by setting a threshold. In the**Decision stage,** the user's claim is either accepted to be genuine or rejected as an imposter depending on the matching score.
Analysis of a biometric system is represented using various parameters. [1][2][3][4] This paper deals with the parameters used to analyze and measure the accuracy of the biometric system. The paper encompasses the requirements for a general biometric system, parameters used in analysis of a biometric system, standard plots used as a reference to measure the parameters, and the experimental results of the palm recognition system using the POLY U database.

2. BIOMETRIC SYSTEM
Biometrics is the measurement of a biological data where a person's authentication is verified by analyzing physical characteristics including face, eyes, and finger print. Any human physiological trait can serve as a biometric as long as it satisfies the requirement of universality that states that every individual possesses a given trait that is measurable. Furthermore, that trait must be unique for every individual. As such, traits between any two individuals should be different in terms of characteristics and permanence, where the parameters used is measurable and denotesthe accuracy of the designed biometric system.

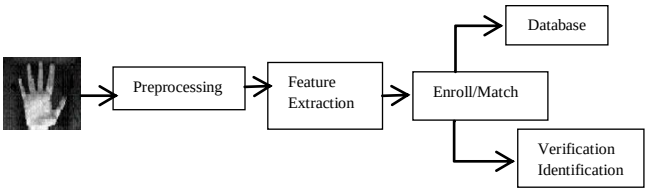

Figure 1: Biometric System

A Biometric system consists of input device, processing stage and a data base. In order to identify an individual any physical trait like face, palm, finger print is captured by input device and preprocessed to store features and later used for matching. The preprocessing stage involves algorithms to convert the features extracted into feature vectors and is stored in the data base. A classifier is trained using these feature vectors which matches the unknown input trait with the stored feature vector using a threshold set for comparison. Matching scores are estimated and input is classified as genuine for maximum matching score, or as imposter for matching score below threshold.

3. PARAMETERS USED TO MEASURE THE PERFORMANCE OF A BIOMETRIC SYSTEM

3.1 Verification: It is one to one matching which involves confirming or denying the claimed identity of a person by comparing with the stored template of the claimed identity and measuring the degree of similarity.

3.2 Identification: It is one to many matchingwhere a person identity is compared with all stored templates of various feature set in a data base and degree of matching is found by a matching score.

3.3 Intra user variability: Variability observed inthe biometric feature set of an individual.e.g.,palm print of a same person being different under different conditions, e.g., variation in position of the palm,skin condition, etc.

3.4 Inter user similarity: Features extracted fromdifferent individual looking similar e.g., identical twins face images, palm features of two individuals looking similar.

Biometric system classifies an individual either as a genuine or as an imposter .The system may make two type of recognition errors, either falsely recognizing an imposter as genuine or by rejecting a genuine user as an imposter resulting to False match and False non match.

3.5 False non match (FNM): when samples ofsame persons biometric trait is not recognized as a match, resulting to false non match. This is due to incorrect interaction of a user with sensor e.g., in-correct position of

a palm with the sensor, incorrect position of a face in front of a camera etc.

3.6 False match (FM): When samples of different persons is incorrectly recognized as a match due to similarity, this results to false match. This is due to larger similarity between two individualse.g., similarity in identical twin faces, similarity in hand writing etc.

3.7 False Rejection rate and false acceptance rate (FRR and FAR): The multiple attemptsdone with the system to enroll or getting rejected is measured by False acceptance rate and False rejection rate FAR is fraction of imposter score > thresh-old FRR is portion of genuine score<threshold. Both FAR and FRR are functions of system threshold, if the threshold is increased then FAR will decrease but FRR will increases and vice versa .So, for a given biometric system both the errors cannot be decreased simultaneously by varying the threshold. The various thresholds used are summarized to mea-sure system performance with the help of ROC and DET plots.

3.8 Genuine acceptance rate: It is the fraction ofgenuine scores that exceeds the threshold.

GAR = 1-FRR

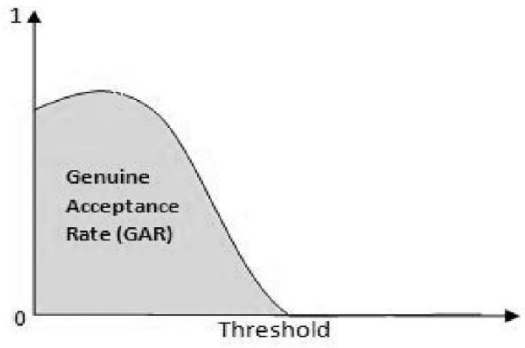

Figure 2: Genuine Acceptance Rate

3.9 Identification rate: The rate at whichclaimants who are in a database, are properly identified.

3.10 Failure to enroll and Failure to capture: If aperson cannot interact properly with the sensor or with the feature extractor the system cannot process which is referred as failure to enroll or failure to capture e.g., poor quality image or improper interaction with the sensor.

3.11 Match score: Classifier compares the featurevectors stored with that of the features extracted from input trait and measures the similarity be-tween two samples by calculating matching scores. Depending on matching scores and input is classified as genuine or imposter.

3.11 ROC PLOT: It is the receiver operating characteristics represented by plotting genuine acceptance rate vs. false acceptance rate.

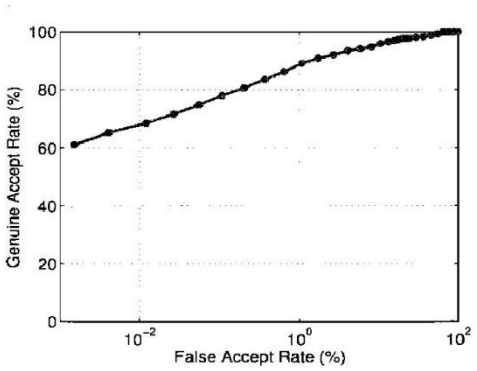

Figure 3: ROC plot

3.12 EER: It is the statistic used to show the biometric performance operating under verification task. The EER is the location on a ROC or DET curve where the false accept rate and false reject rate are equal. In general, lower the equal error rate value,the higher the accuracy of the biometric system. The EER is sometimes referred to as the Crossover Error Rate.

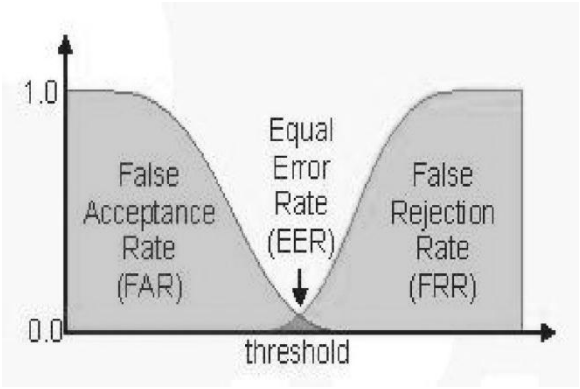

Figure 4: Equal Error Rate

DET: A graphical plot showing a false match rateand false non match rate by varying a threshold. The DET summarizes the verification performance of the biometric algorithm on the samples on which it is calculated.

CMC: Another performance measure of a biometric system is given by CMC (cumulative match characteristic) that ranks biometric templates of all users in the database based on their relative accuracy in authentication. As a performance indicator CMC provides a qualitative comparison among biometric templates for all users.CMC does not give much idea on inter-relation of users based on their biometric information nor does it provide a measure of the information content in biometric features or in matching scores.[9][10][11][12][15]

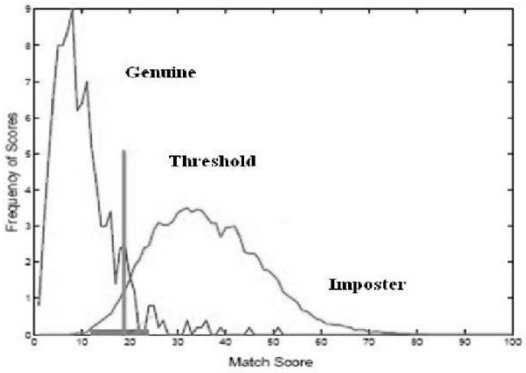

Figure 5: Performance Plots

4. EXPERIMENTS

To evaluate the performance of palm print recognitionsystem, POLY U data base with 600 images of 100 individuals is used. Palm is used as reliable, cost effective, easily acquired person identificationmodality. The inner palm surface consists of many unique features such as principal lines, ridges, wrinkles, and delta points, which are to be extracted and matched with a larger data set.[5] Initially low pass filter was applied on the image to remove the noise. To distinguish the palm image from the background it is converted to binary image using histogram analysis method.

F(x,y) = 255 if f(x,y) _ Gray level.
F(x,y) = 0 if f(x,y) _ Gray level.

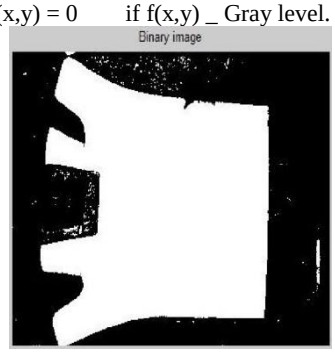

Figure 6: Binary Image

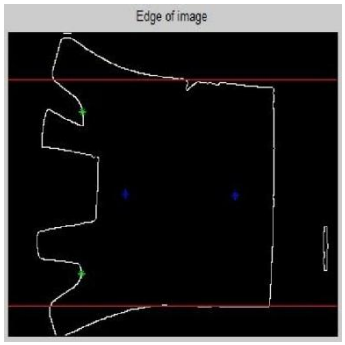

Figure 7: Region of Interest Extraction

4.1REGIONOF INTEREST (ROI)

Align a specified area and scan the binary image to t into it. Select a point P on the palm edge on the X axis and decrement it at specified levels in row wise. Select another point from the bottom edge on the Y axis at same level of P and increment it row wise. If the decrement level is equal to increment level, the outward image is cropped. The procedure is repeated for Y axis point selected on the palm edges. Again assigning a new area specified the entire process is repeated till weend up with centerarea of the palm. The center of the palm is cropped for feature extraction.

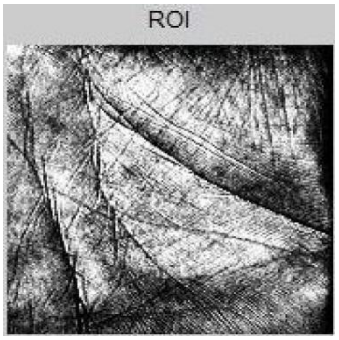

Figure 8: Cropped image of the center palm

4.2 FEATUREEXTRACTION

Features of the cropped image are extracted using multi scale edge detection with wavelet transform.Edges in the image are mathematically defined as local singularities. Wavelet transform is a mathematical tool to analyze the singularity. The maxima of the wavelet transform module can detect the location of the irregular structures. For an image F(x,y) its edges corresponds to singularities of F(x,y). The image is first smoothed by smoothing filter and its gradient is computed by gradient operator.

$$\left|\left|\nabla f\right|\right|_2 = \sqrt{f_x^2 + f_y^2}$$

The local maxima is a point f(x; y) which is an edge point of an image F(x,y) andin the neighborhood

$$\left|\left|\nabla f(\bar{x},\bar{y})\right|\right| > f(x,y)$$

. An edge curve in an image is a continuous curve on which all points are edge points and a set of all edge points is an edge image.

$$\max\left|\left|\nabla f(\bar{x},\bar{y})\right|\right| = M$$

The edge threshold is set as choosing k,such that $0 < k < M$. If $\left|\left|\nabla f(\bar{x},\bar{y})\right|\right| \geq k$then $(\bar{x},\bar{y})$ is called edge point of F(x,y). Then the smoothing function Φ(x), waveletΨ(x) are built. All kinds of edges like step edge, smoothed edge, Dirac edge, fractal edge, can be detected using wavelet transform. The sharpness of the edge is found by Lipschitz exponent. To separate real edges from false edges a threshold is used.[6][7][10][13][14]

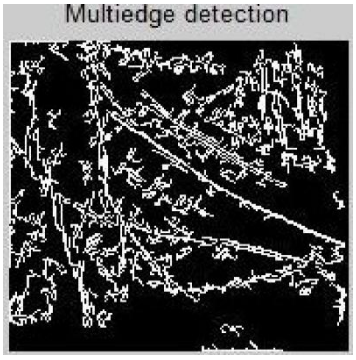

Figure 9: Multi-edge Detection

4.3 MATCHINGAND DECISION MAKING

Template matching compares a portion of image with one another. The matching process involves correlating pixels

by pixels of images by using correlation function

$$Cor_{x,y} = \frac{\sum_{i=0}^{N-1}(x_i - \bar{x}) * (y_i - \bar{y})}{\sqrt{\sum_{i=0}^{N-1}(x_i - \bar{x})^2 * \sum_{i=0}^{N-1}(y_i - \bar{y})^2}}$$

The computation score is given by matching score. [8]By setting a threshold the degree of accuracy is estimated. The experiment is carried out by setting various threshold and the parameters are measured and plotted. It is observed that there exists a maximum accuracy with minimum error at a set threshold value. The plots of EER, FAR, GAR, and FRR are plotted and as shown.

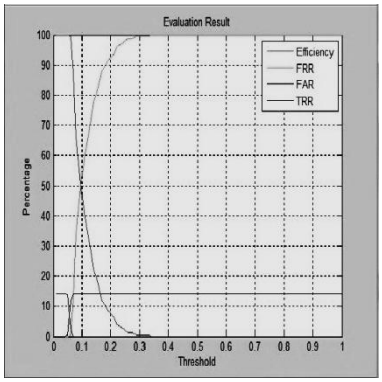

Figure 10: ROC Plot

5. CONCLUSION

An accurate biometric systems depends on various factors like image acquisition depending on the application i.e.,high resolution or a low resolutionimage, Preprocessing to extract ROI which defines the features of the palm and is having unique features, feature extraction algorithm to extract the features of the region of interest,a mapping algorithm to correlate the given image with that of the data base image and finally a classifier to decide if the given input is of genuine or of an imposter.In addition to these factors the various parameters are used to measure the overall performance of the biometric system.

6. REFERENCE

[1] A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics. Springer Verlag, 2006

[2] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. L. Wayman, Biometrics: A Grand Challenge, Proc. ICPR, vol. II, UK, pp. 935-942, 2004.

[3] A. K. Jain, A. Ross, and S. Pankanti, Biometrics: A Tool for Information Security, IEEE Trans. on Information Forensics and Security, vol. 1, no. 2, pp. 125-143, 2006.

[4] A. Adler, R. Youmaran, and S. Loyka, Towards a measure of biometric information, Proc. Canadian Conf. Computer Elec. Eng., CCECE, Ottawa, Canada, 2006.

[5] http://www.sce.carleton.ca/faculty/adler//publications.

[6] A. Kumar and D. Zhang, Personal authentication using multiple palm print representations, Pattern Recognition, vol. 38, pp. 1695-1706, Oct. 2005.

[7] A. Ross, and A. K. Jain, Information Fusion in Biometrics, Pattern Recognition Letters, vol. 24, no.13, pp.2115-2125, 2003.

[8] A. Kumar and D. Zhang, Personal recognition using shape and texture, IEEE Trans. Image Process., vol. 15, no 8, pp. 2454-2461, Aug. 2006.

[9] G. Aggarwal, N. Ratha, and R. M. Bolle, Bio-metric Verification: Looking Beyond Raw Similarity Scores, Workshop on Multibiometrics (CVPR), New York, pp. 31 36, 2006

[10] J. Bhatnagar and A. Kumar, On Some Performance Indices for Biometric Identification Sys-tem, Proc. ICB 2007, Lecture Notes in Computer Science, Springer-Verlag GmbH, vol. 4642, pp. 1043-1056, Aug. 2007.

[11] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio (Eds.), Biometric Systems: Technology, Design and Performance Evaluation. New York: Springer Verlag, 2005.

[12] N. A. Schmidt and J. A. O'Sullivan, Performance Prediction Methodology for Biometric System Using Large Deviations Approach, IEEE Trans. Signal Processing: Supplement on Secure Media, vol. 52, no. 10, pp. 3036-3045, 2004.

[13] N.A. Schmidt; M.V. Ketkar, H. Singh, and B. Cukic, Performance analysis of iris-based identification system at the matching score level,IEEE Trans. on Information Forensics and Security, vol. 1, no. 2, pp. 154-168, 2006.

[14] S. Dass, K. Nandakumar, and A. K. Jain, A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, Proc. AVBPA, pp. 1049-1058, New York, 2005.

[15] Y. Zhu, S.C. Dass and A.K. Jain, Statistical Models for Assessing the Individuality of Fingerprints, IEEE Trans. on Information Forensics and Security, vol. 2, no. 3, pp. 391-401, 2007.

[16] W.Feller, An Introduction to Probability Theory and Applications. John Wiley & Sons, 1971.