Available Online at www.ijecse.org **ISSN- 2277-1956**

A Multimodal Biometric Recognition System based on Fusion of Palmprint, Fingerprint and Face

Mrs.Asmita S.Deshpande [1] , Mr.S.M.Patil [2] Mrs.Rekha Lathi [3]
[1 2] Department of Information Technology
[1]Assistant Professor, PCTCOE, Thane
[2] HOD, IT, BVCOE, Kharghar
[3]Asst.Professor,Computer Dept,PIIT,Panvel
[1] asdeshpande18@gmail.com,smpatil2k@gmail.com, [3]rekha_lathi@yahoo.com

Abstract- Multibiometric recognition systems, which aggregate information from multiple biometric sources, are gaining popularity because they are able to overcome limitations such as non-universality, noisy sensor data and susceptibility. Multibiometric systems promise significant improvements as higher accuracy and increased resistance to spoofing over the single biometric systems. This paper proposes a method which integrates fingerprint, palmprint and face and performs the fusion at score level. Three biometric traits are collected and stored into database at the time of Enrollment. In the Authentication stage query images will be compared against the stored templates and match score is generated.AOV based minutiae algorithm is proposed for fingerprint matching. To compare Face images PCA analysis is used. Palmprint matching score can be generated using PCA analysis. This matching score will be passed to the fusion stage. Fusion stage includes normalization of the scores. Weights can be assigned according to the importance of the biometric traits. These weighted and normalized score will be combined to generate a total score. This total score will be passed to the decision stage. In the decision stage total score will be compared with certain threshold value. That will realize person's authenticity whether a person is genuine or imposter.

Keywords – Multibiometric, fingerprint, palmprint, face, AOV,PCA

I. INTRODUCTION

In the recent years, biometric authentication has become popular in modern society. Multimodal biometric person authentication systems integrate multiple authentication techniques, and are important for many security applications such as government, defense, surveillance and airport security. Biometrics is defined as the science of recognizing an individual based on his/her physical or behavioral property [1]. As password or PIN can lost or forgotten, biometrics cannot be forgotten or lost and requires physical presence of the person to be authenticated. Thus personal authentication systems using biometrics are more reliable, convenient and efficient than the traditional identification methods. Multimodal biometrics has become increasingly important, particularly because single modal biometrics has reached its bottleneck; i.e. non-universality, noise in sensor data and spoofing. Multimodal biometrics gives supplementary information between different modalities that increases recognition performance in term of accuracy and ability to overcome the drawbacks of single biometrics. There are two types of biometric techniques: Physiological (face recognition, iris recognition, and finger print recognition). And the other one is Behavioral (signature recognition, gait, voice recognition). In this paper we concentrate on the physiological features such as fingerprint recognition, face recognition and palmprint recognition. Authentication by using multimodal biometrics offers high reliability due to the presence of multiple piece of evidence and it is more difficult to simultaneously forge multiple biometric characteristics than to forge a single biometric characteristic.[2].

II. SYSTEM DESCRIPTION

A generic biometric system operates in two stages one is the capture and storage of enrollment biometric samples and the capture of new biometric samples and their comparison with corresponding reference samples. The proposed Multimodal Biometric Authentication system works in a six-stage process that consists of the following stages.

- Image Capture
- Image Preprocessing
- Feature Extraction
- Matching
- Fusion
- Decision

A. Image Capture Stage

A multimodal biometric authentication system collects the samples of biometric features. In the proposed system we capture the images of fingerprint, palmprint and face who wants to register in the system. To capture the face image and palm high quality webcamera is used. Fingerprint images are captured using optical fingerprint reader. Fingerprint image size will 260*300 pixels and the image size for face and palm will be 320*240 pixels.

B. Image Preprocessing

The images must be preprocessed before going for the next stage. Image preprocessing is done with the intention of removing unwanted data in the image such as noise, reflections.The objective of image processing stage is to filter, binarize, enhance and skeletonize the original gray-level image.In the proposed system we have to preprocess three images obtained by three various biometric traits.

C. Fingerprint Image Preprocessing

Fingerprints are texture on the top of human fingertip. Fingerprint is a graphical flow-like ridges present on human fingers.[3].It has been widely used for person identification for several centuries.The fingerprint is basically the combination of ridges and valleys on the surface of the finger. The lines that create fingerprint pattern are called ridges and the spaces between the ridges are called valleys or furrows. In the context of fingerprint, minutiae refer to various ways that the ridges in a fingerprint can be discontinuous. The goal of fingerprint image preprocessing is to increase the clarity of ridge structure so that minutiae points can be easily and correctly extracted. Figure 1 indicates the preprocessing stage for fingerprint.

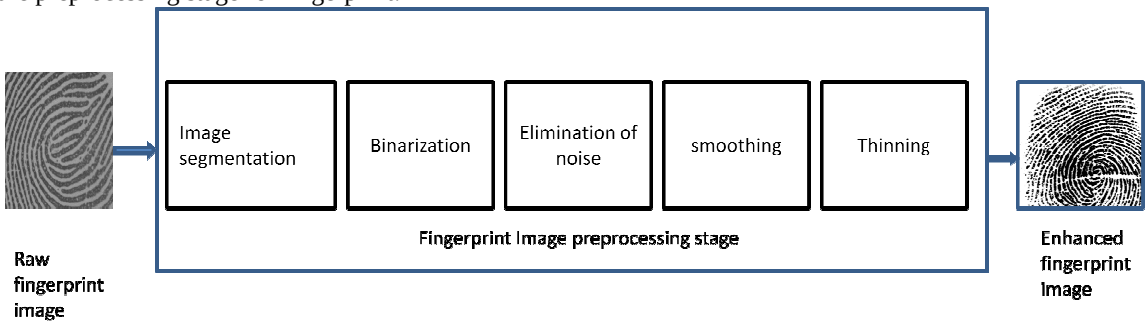

Figure 1Fingerprint Image Preprocessing

Once a high-quality image is captured, there are several steps required to convert its distinctive features into a compact template.. The above image preprocessing steps are sequentially applied to achieve the enhanced image. Image preprocessing is applied for images at the time of enrollment as well as authentication.

D. Face Image Preprocessing

Faces differ in thousands ways because of the differences in shape, size and structure of the organs. In general, face recognition techniques can be divided into two groups based on the face representation they use one is Appearance-based, which uses holistic texture features and is applied to either whole-face or specific regions in a face image. and the other one is Feature-based, which uses geometric facial features and geometric relationships between them. At the time of enrollment face image is captured by using web camera. These images will undergo image processing stage. After image preprocessing enhanced face image will be passed to the fusion stage. Figure 2 indicates the preprocessing steps for face.

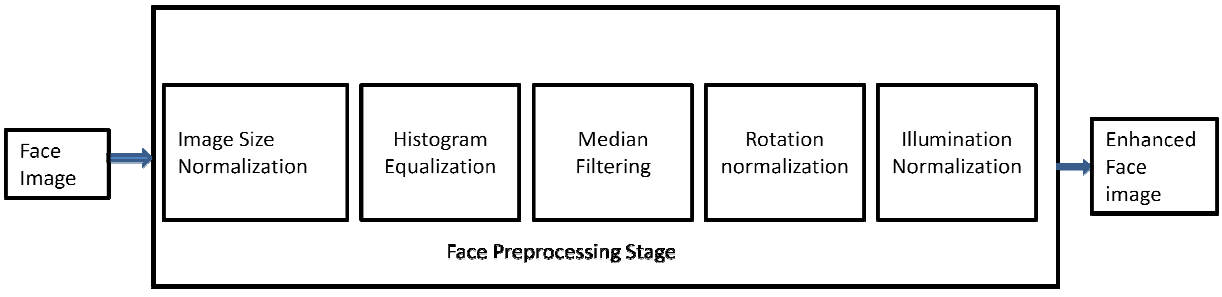

Figure2:Face Image Preprocessing

E. Palmprint Image Preprocessing

Palmprint is one of the relatively new physiological biometrics due to its stable and unique characteristics. The area of the palm is much larger than the area of a finger and as a result, palmprints are expected to be more distinctive than the fingerprints. Unique features of the palm-print include principle lines, wrinkles, ridges and datum points. There are two approaches for palmprint recognition, one is transforming the palmprint images into specific transformation domains and the other one is to extract principal lines and creases extracted from ROI [4,5].Palmprint image is acquired using a high quality webcamera and subsequently undergoes under preprocessing steps as shown in figure 3.

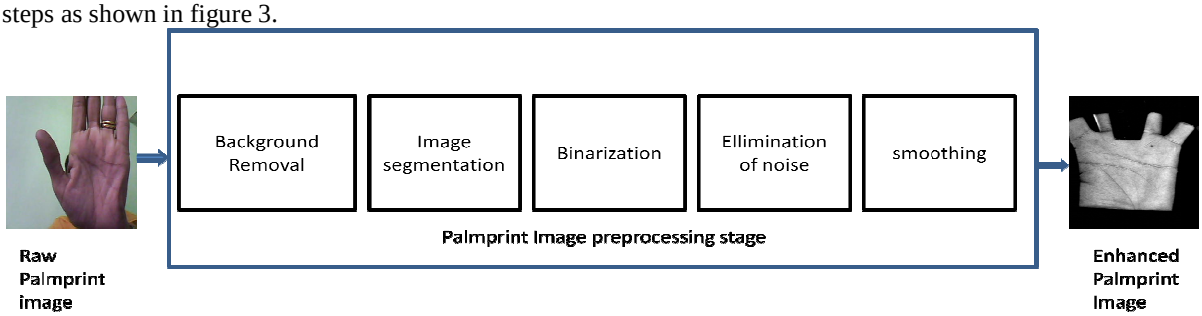

Figure. 3:Palmprint Image Preprocessing Stage

F. Feature Extraction Stage

a. Minutiae extraction

Minutiae points are essentially the endings and bifurcations of the ridgelines that constitute a fingerprint. The minutia can be represented by the type, position and orientation. The minutiae type can be either ridge ending or ridge bifurcation. The direction of a minutia is, in this system, defined to be the angel of the vector that starts in the minutia and ends in the eight pixel of the ridge that the minutia belongs to. The location of minutiae points along with the orientation is extracted and stored to form a feature set. Fingerprint matching techniques can be placed into two categories: minutiae based and correlation based.[6]. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Fingerprint matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns. The extraction of minutiae points is a difficult step in fingerprint recognition system. This is when the fingerprint information captured by the scanning device is transformed to a format that can be matched by an automated system. The feature vector of minutia generally consists of the minutia type, the coordinates and the tangential angle of the minutia. The minutia correspondences are difficult to obtain due to several factors such as the rotation, translation and deformation of the fingerprints, the location and direction errors of the detected minutiae as well as the presence of spurious minutiae and the absence of genuine minutiae. Adjacent feature of a minutia is very important for matching because it is rotation invariant and translation invariant. In this paper, we will present a fingerprint minutiae matching by using Adjacent Orientation Vector (AOV).

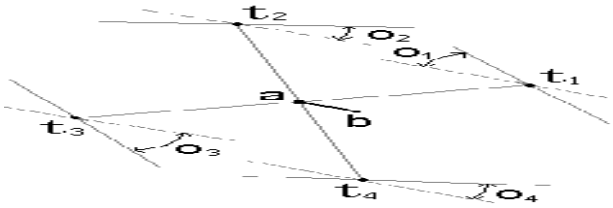

Figure4:Illustration of adjacent orientation vector [7]

Fig.3 depicts how to find adjacent orientation vector. If a is a minutia of a fingerprint, then b is the corresponding orientation point, whereas c, d, e and f are the four adjacent minutiae satisfying |ac|=|ad|=|ae|=|af|=D,<bac=0 , <bad =π, bae=π, and <baf =3π/ 2 where D is a constant. Since a, b, c and d are four points in the fingerprint image, there will be certain orientation at the four Points. We assume the difference between the four orientations and minutiae orientation are 1 o , 2 o ,3 o and 4 o respectively. The ridge number between ac, ad, ae and af is also used to ensure

reliable matching, which is named as 1 n , 2 n , 3 n and 4 n respectively. The vector < 1 o , 2 o , 3 o , 4 o , 1 n ,2 n , 3 n , 4 n > is named AOV.[7].Assume direction of a is ϕ, then o1=$\theta 1 - \phi$, o2=$\theta 2 - \phi$, o3=$\theta 3 - \phi$, o4=$\theta 4 - \phi$. Now these o1, o2, o3, o4 are rotation and translation invariant. Now AOV for point a can be calculated as AOV(a)=<oa1,oa2,oa3,oa4,na1,na2,na3,na4>. Let AOV(x) and AOV(y) denotes the vectors for different minutiae x and y.By using Euclidean distance formula the similarity can be measured between these two minutiae points.

b. Face feature extraction

The feature extraction module for face composes a feature vector that is well enough to represent the face image. Eigenfaces approach seemed to be an adequate method to be used in feature extraction due to its simplicity, speed and learning capability. Eigenfaces are a set of eigenvectors used in human face recognition. They seek to capture the variation in a collection of face images and use this information to encode and compare images of individual faces. Eigenfaces are the principal components of a distribution of faces, or equivalently, the eigenvectors of the covariance matrix of the set of face images [7].Eigenfaces are mostly used to extract the relevant facial information and to represent face images efficiently by reducing time and space complexity. The training set of images is given as input to find eigenspace. Using these images, the average face image is computed. Covariance matrix represents the difference of these images with respect to the average face image. Eigenvectors and Eigenvalues can be calculated accordingly. These are the Eigenfaces which represent various face features. Eigenvalues are sorted and higher of them which represent maximum variations will be considered. This becomes eigenspace spanned by the eigenfaces, which has lower dimension than original images. PCA is used to extract linear features from the original input images by transforming a set of m variables (high dimensionality) to a set of n variables by maintaining as many variances of the original data as possible [8]. The feature vector of a face image is the projection of the original face image on the reduced eigenspace. This feature vector is stored as a template in the system database.

c. Palmprint Feature Extraction

Gabor transformation can capture prominent visual properties. Gabor filter can be used to extract the rich line features of palmprint. Palmprint is more reliable biometric feature at it covers larger area than the fingerprint. The rich line features remain unaltered throughout the person's life. In this paper PCA approach can be used which transforms palmprint images into specific transformation domains to find useful image representations in compressed subspace. It computes a set of basis vector from a set of palmprint images, and the images are projected into the compressed subspace to obtain a set of coefficients called as eigenpalms.[8].

G. Matching Stage

At the time of Enrollment, fingerprint, palmprint and face images will be acquired. Feature vectors are generated for each biometric trait and stored separately in the system database. At the time of authentication, when user wants to prove his/her identity fingerprint image will be acquired by using optical fingerprint reader. Face and Palmprint image will be captured using web camera. These images again will undergo image preprocessing and feature extraction stage. Template will be compared with the respective template created at the time of Enrollment. The minutiae based matching consists of finding alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings [6]. This pairing generates a similarity score (MS_1). Euclidean distance formula is used to compute the distance between the eigenpalm coefficients of the template and the query palm image. This will generate score MS_2. Euclidean distance formula is used to compute the distance between the template and query face image. Match scores MS_3 is generated. All these three scores will be passed to the fusion stage. Fingerprints are represented using minutiae features, and the output of the fingerprint matcher is a similarity score. Face images are represented using eigen-coefficients, and the output of the face matcher is a distance score. Palmprint images are represented using eigenpalm-coefficients, and the output of the palmprint matcher is a distance score.

H. Fusion Stage

MS_1, MS_2 and MS_3 are the matching scores generated by fingerprint, palmprint and face recognizers respectively. Since the matching scores output by the three traits are heterogeneous because they are not on the same numerical range, so score normalization is done to transform these scores into a common domain prior to combining them [9].Total score TS is generated by using weighted sum rule, which will passed to the decision stage.

I. Decision Stage

Total score TS will be compared against the set threshold value. This will decide whether the person is genuine or imposter.In this system we have given equal weights to all biometric traits, i.e.face,fingerprint and palmprint.We can change the weights of the individual modality according the modality for which we can find best results.

III. SYSTEM ARCHITECTURE

Following diagram indicates the functional block Diagram.

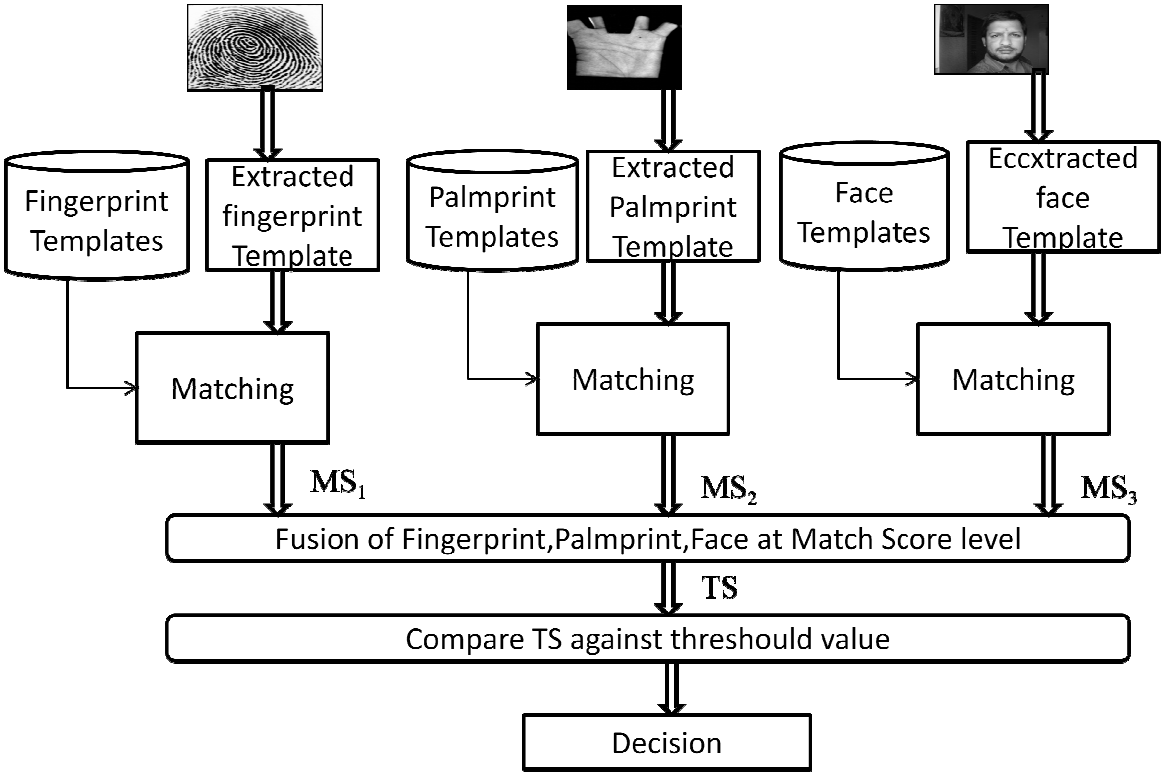

Fig.5. Functional Block Diagram Indicating Fusion of Fingerprint,Palmprint and Face at Match Score Level.

IV. CONCLUSION

Biometric systems are widely used to overcome the traditional methods of authentication. But the unimodal biometric system fails in case of biometric data for particular trait. Thus the individual score of three traits (face & palmprint, fingerprint) are combined at classifier level and trait level to develop a multimodal biometric system. Multimodal system performs better as compared to unimodal biometrics with accuracy of more than 98%.

REFERENCES

[1] Jain, A.K., Ross, A., Pankanti, S. "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, vol. 1,Issue: 2, June 2006, pp: 125-143.

[2] Zhang "Biometric solutions for authentication in an eworld",Kluwer Academic Publishers, 2002.

[3] Almudena Lindoso, Luis Entrena, Judith Liu-Jimneez, Enrique San Milan, "Increasing security with correlation based finger printing", 41st annual IEEE International carnahan Conference on security technology, 8-11 October 2007.

[4] Lu. G., David. Z., and Wang. K.. Palmprint recognition using eigenpalms features. Pattern Recognition Letters, 24(9-10), pp. 1473-1477, 2003.

[5] Wai. K.K., David. Z., and Li. W.. Palmprint feature extraction using 2-D Gabor filters. Pattern Recognition, 36(10), pp. 2339-2347,2003

[6] X. Jiang and W. Y. Yau. Fingerprint minutiae matching based on the local and global structures. Proc. ICPR2000, 2:1042-1045, Sep, 2000

[7] X. Tong, J. Huang, X. Tang and D. Shi, Fingerprint Minutiae Matching Using Adjacent Feature Vector

[8] G. Feng, K. Dong, D. Hu & D. Zhang, When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy, ICBA, pp. 701-707, 2004

[9] S. C. Dass, K. Nandakumar & A. K. Jain, A principal approach to score level fusion in Multimodal Biometrics system, Proceedings of ABVPA, 2005