Hybrid Fusion based Multimodal Biometric System for Accurate Personal Identification

Dr.D. Maheswari and B. Parameswaran

Abstract--- In the recent years, biometric authentication has become popular in modern society. The recognition accuracy of unimodal biometric systems has to contend with a variety of issues such as background noise, noisy data, non-universality, spoof attacks, intra-class variations, inter-class similarities or distinctiveness, interoperability problems. To overcome the limitation of a single biometrics, information from multiple biometrics can be integrated to achieve more reliable and robust performance. In existing system, score level fusion method is introduced to achieve better identification result using Left and Right Palmprint Images. However, various normalization methods of the matching scores cause different decision boundaries. Also, a too small training set of scores might easily overfits the data, especially in methods with flexible boundaries. To solve this problem, the proposed system introduced a hybrid fusion approach which integrate both score level and decision level fusion. In this proposed system, left and right palmprint of the same subject is correlated and crossing matching score of the left and right palmprint is computed for improving the efficiency of identity identification. Then ROC is derived from the component matching scores and the score-level fused matching scores. Finally combined both score level and decision level results to achieve hybrid fusion. The experimental results show that the proposed system achieves better performance compared with existing system in terms of detection rate and false acceptance rate.

Keywords--- Multimodal Biometric, ROC, Hybrid Fusion.

Dr.D. Maheswari, Head & Research Coordinator, School of Computer Studies, PG Rathnavel Subramaniam College of Arts and Science, Coimbatore.
B. Parameswaran, Asst. Prof., Department of Computer Science & Applications, Providence College for Women, Coonoor. E-mail: paramprovidence@gmail.com

I. INTRODUCTION

Biometric authentication has been receiving much interest over the past decade with rising demands in automated personal identification [1]. A biometric authentication system is basically a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological and/ or behavioral characteristic possessed by the user [2]. Physiological characteristics are related to the shape of the body, such as hand geometry, Palm print; face recognition, fingerprint, DNA, iris recognition, retina and odor. Behavioral characteristics are related to the behavior of a person, such as typing rhythm, gait, and voice. The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time of identification and identification based on biometric techniques obviates the need to remember a password or carry a token. Since, today, a wide variety of applications require reliable verification schemes to confirm the identity of an individual, recognizing humans based on their body characteristics became more and more interesting in emerging technology applications [3] [4].

Biometric Systems

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.

Depending on the application context, a biometric system may operate either in verification mode or identification mode [5]:

In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "Does this biometric data belong to Bob?"). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity [6].

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity(e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be [7].

The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics [8] [9].

Need for Palmprint Technology

Biometrics has been an emerging field of research in the recent years and is devoted to identification of individuals using physical traits, such as those based on iris or retinal scanning, face recognition, fingerprints, or voices. As unauthorized users are not able to display the same unique physical properties to have a positive authentication, reliability will be ensured. Palmprint is preferred compared to other methods such as fingerprint or iris because it is distinctive, easily captured by low resolution devices as well as contains additional features such as principal lines. Iris input devices are expensive and the method is intrusive as people might fear of adverse effects on their eyes. Fingerprint identification requires high resolution capturing devices and may not be suitable for all as some may be finger deficient. Palmprint is therefore suitable for everyone and it is also non-intrusive as it does not require any personal information of the user. Palmprint images are captured by acquisition module and are fed into recognition module for authentication.

Compared with face recognition palmprint is hardly affected by age and accessories. Compared with fingerprint recognition palmprint images contain more information and needs only low resolution image capturing devices which reduces the cost of the system.

Compared with iris recognition the palmprint images can be captured without intrusiveness as people might fear of adverse effects on their eyes and cost effective

Palm Print

Palmprint is the inner part of a person's hand. For centuries, the palm line patterns have popularly been believed to be able to predict a person's future. But its uniqueness and capacity for distinguishing individuals has come to fore only recently. Palmprint is also one of the reliable modality since it possess more features than that of the other modality such as principal lines, orientation, minutiae, singular points etc. Also palmprint modality is unique for each individual, moreover it is universal[9] [10].

Palmprint recognition is used in civil applications, law enforcement and many such applications where access control is essential. Palm has features like geometric features, delta point's features, principal lines features, minutiae, ridges and creases. Principal lines are namely heart line, head line and life line.

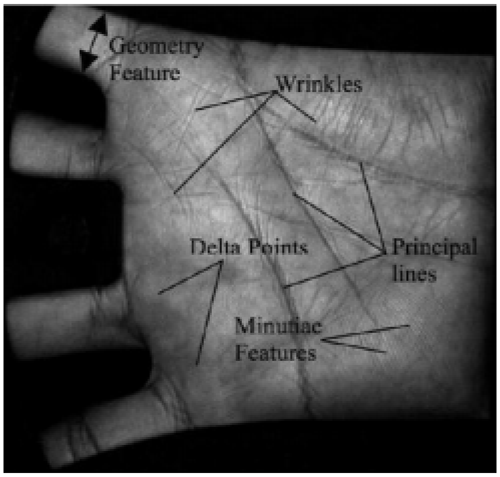

Figure 1: Different Features of Palm

Figure 1 shows structure of palmprint. Palmprint contains three principal lines which divides palm into three regions: Interdigital, Hypothenar and Thenar. An Interdigital region lies above the Heart line. The Thenar lies below the Life line. And Hypothenar is between Heart and Life line. From palmprint principal lines, minutiae, ridges features can be extracted for identification [11] [12].

Overview of Palmprint Recognition

Image acquisition, preprocessing, feature extraction, and identification in enrollment process, several palmprint samples have to be given by the user to the system. Verification is the process of comparison with only those templates corresponding to the claimed identity [13] [14].

Identification is the process of comparing the palmprint against templates corresponding to all users in the database [15] [16]. Palmprint identification as wide application is used in both off-line applications as well as in on-line applications. In the case of off-line applications mainly high resolution images are used. Off-line applications include criminal detection [17] 18] [19]. On-line applications like civil and commercial application use low resolution images.

II. LITERATURE SURVEY

Happy et.al [20] introduced a face recognition method which is based on hybrid local features. In this work select the suitable block size, weights and distance classifiers for optimal classification results using LBP on various face databases. After the selection of best performance by using specific LBP, then investigate this LBP from a different perspective of information fusion scheme. The first feature set is derived by local binary pattern which is fed to histogram intersection classifier. The second feature set is obtained by extracting statistical features from local regions after the division procedure, and then it is forwarded to city block distance classifier. Finally, decision level fusion scheme is used to fuse the results from individual algorithm. The recognition is evaluated using different similarity measures on public face databases.

Badrinath et.al [21] introduced a Stock well transform based palm-print recognition. A technique to encode the palm-print binarising the variation of instantaneous-phase of local region obtained using Stock well transform (ST) is proposed. Phase of ST instead of magnitude is used because of its inherent stability. Phase does not depend on intensity levels of the image. Hence, measurements are invariant to smooth shading and lighting conditions. The instantaneous-phase using ST of radically averaged overlapping circular-strips from the normalized and non-uniform brightness corrected palm-print is extracted. Instantaneous-phase difference from subset of overlapping circular-strips is binarised with the help of zero crossing on the instantaneous-phase difference to generate binary features. Nearest-neighbour approach is used for identification with Hamming distance to measure the similarity. Based on this palm-print is recognized.

Han et.al [22] introduced a Personal authentication mechanism using palm-print features. In this work, a scanner-based personal authentication system is introduced. The authentication system consists of enrollment and verification stages. In the enrollment stage, the training samples are collected and processed by the pre-processing, feature extraction, and modeling modules to generate the matching templates. In the verification stage, a query sample is also processed by the pre-processing and feature extraction modules, and then is matched with the reference templates to decide whether it is a genuine sample or not. The region of interest (ROI) for each sample is first obtained from the pre-processing module. Then, the palm-print features are extracted from the ROI by using Sobel and morphological operations. The reference templates for a specific user are generated in the modeling module. Finally use the template-matching and the back propagation neural network to measure the similarity between the reference templates and test samples.

Ibrahim et.al [23] presents a robust palm print verification system based on evolution of Kernel Principal Component Analysis. A new approach in feature extraction called evolution of kernel principal component analysis (Evo-KPCA) was proposed to speed up the processing time in the extraction stage. It used a reduced set density estimate (RSDE) to define a weighted gram matrix. The support vector machine (SVM) employed to calculate the score of the between training and testing data.

Biradar et.al [24] introduced a new Personal Identification mechanism Using Palm print Biometrics Based on Principal Line Approach. In preprocessing a Gaussian filter is used to smooth the image and next ROI is extracted based on valley points. The Canny edge detection operation is proposed to extract principal line features. The edge direction and gradient strength of each pixel in the preprocessed image are found using Sobel masks. Then edges are traced using that information. Finally, non-maximum edges are suppressed by finding parallel edges and eliminating those with weaker gradient strengths. In this way principal lines are extracted and resultant image is obtained. The matching is done by dividing the resultant image into 9X9blocks. The blocks are traced to create feature vector. While generating a template the feature vector bit is set if the concerned block contains the line. Personal identification is done based on the distance matching between the stored templates and the test palmprint image.

Imtiaz et.al [25] introduced a wavelet-based dominant feature extraction algorithm for palm-print recognition. The system implemented to extract precisely spatial variations from each local zone of the entire palm-print image instead of concentrating on a single global variation pattern. In this palm-print recognition scheme, the entire palm-print image of a person is segmented into several small modules. The effect of modularization in terms of the entropy content of the palm-print images has been investigated. A wavelet domain feature extraction algorithm using 2D-DWT is developed to extract dominant wavelet coefficients corresponding to the spatial modules residing within the image. In the selection of the dominant features, a threshold criterion is proposed, which not only drastically reduces the feature dimension but also captures precisely the detail variations within the palm-print image. For the task of classification, an Euclidean distance based classifier has been employed to provide a very satisfactory recognition performance.

III. EXISTING METHODOLOGY

Multibiometrics can provide higher identification accuracy than single biometrics, so it is more suitable for some real-world personal identification applications that need high-standard security. Among various biometrics technologies palmprint identification has received much attention because of its good performance. Combining the left and right palmprint images to perform multi biometrics is easy to implement and can obtain better result. First, it for the first time shows that the left and right palmprint of the same subject are somewhat correlated, and it demonstrates the feasibility of exploiting the crossing matching score of the left and right palmprint for improving the accuracy of identity identification. Second, it presents an elaborated framework to integrate the left palmprint, right palmprint, and crossing matching of the left and right palmprint for identity identification. Third, it conducts extensive experiments on both touch-based and contactless palmprint databases to verify the introduced framework.

Similarity between the Left and Right Palmprints

In this section correlation between the left and right palmprints is presented. The palmprint images of four subjects are taken. This means four left palmprint images and four right palmprint images of the same four subjects. Fig. 5 shows palmprint images of four subjects

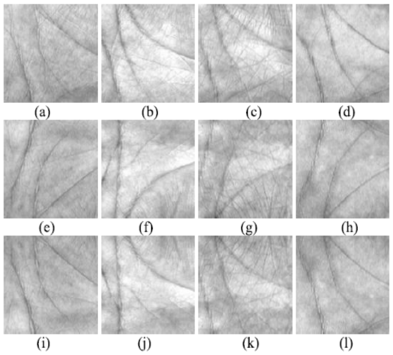

Figure 2: Palmprint Images of Four Subjects

(a)-(d) are four left palmprint images; (e)-(h) are four right palmprint corresponding to (a)-(d); (i)-(l) are the reverse right palmprint images of (e)-(h).

Fig. 2 (a)-(d) show four left palmprint images of these four subjects. Fig. 2 (e)-(h) show four right palmprint images of the same four subjects. Images in Fig. 2 (i)-(l) are the four reverse palmprint images of those shown in Fig. 2 (e)-(h).

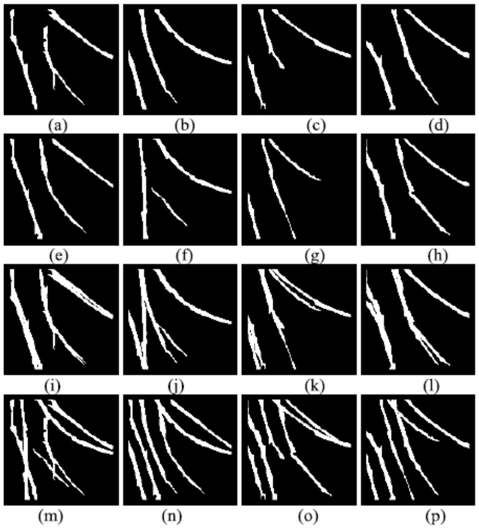

Figure 3: Principal Lines Images

(a)-(d) are four left palmprint principal lines images, (e)-(h) are four reverse right palmprint principal lines image, (i)-(l) are principal lines matching images of the same people, and (m)-(p) are principal lines matching images from different people.

Fig. 3 (a)-(d) depict the principal lines images of the left palmprint shown in Fig. 2 (a)-(d). Fig.3 (e)-(h) are the reverse right palmprint principal lines images corresponding to Fig.3 (i)-(l). Fig.3 (i)-(l) show the principle lines matching images of Fig. 6 (a)-(d) and Fig. 3 (e)-(h), respectively. Fig. 3 (m)-(p) are matching images between the left and reverse right palmprint principal lines images from different subjects. The four matching images of Fig3 (m)-(p). It can be seen that the left palmprint image and the reverse right palmprint image of the same subject are somewhat similar. The principal lines of the left and reverse right palmprint from the same subject have very similar shape and position.

However, principal lines of the left and right palmprint from different individuals have very different shape and position. This demonstrates that the principal lines of the left palmprint and reverse right palmprint can also be used for palmprint verification/identification.

Score Level Fusion Framework

The framework first works for the left palmprint images and uses a palmprint identification method to calculate the scores of the test sample with respect to each class. Then it applies the palmprint identification method to the right palmprint images to calculate the score of the test sample with respect to each class. After the crossing matching score of the left palmprint image for testing with respect to the reverse right palmprint images of each class is obtained, the proposed framework performs matching score level fusion to integrate these three scores to obtain the identification result. The method is presented in detail below.

It suppose that there is C subjects, each of which has m available left palmprint images and m available right palmprint images for training. Let X_i^k and y_i^k denote the i