# 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.

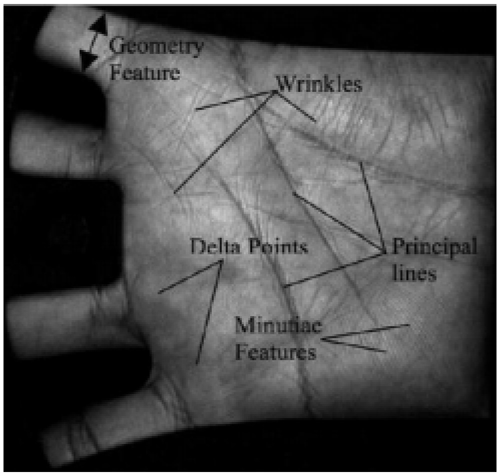


Figure 1: Different Features of Palm

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

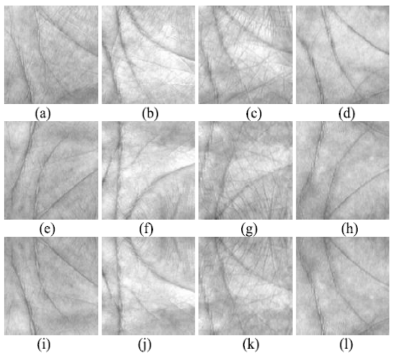

Figure 2: Palmprint Images of Four Subjects

(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).

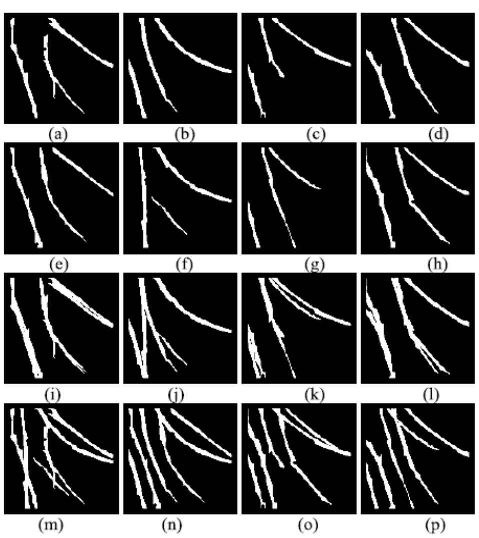

Figure 3: Principal Lines Images

(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 $i$

th left palmprint image and $i$ th right palmprint image of the $k$th subject respectively, where $i = 1, \ldots, m$ and $k = 1, \ldots, C$. Let $Z_1$ and $Z_2$ stand for a left palmprint image and the corresponding right palmprint image of the subject to be identified. $Z_1$ and $Z_2$ are the so-called test samples.

Step 1: Generate the reverse images $\breve{Y}_i^k$ of the right palmprint images $Y_i^k$ . Both $Y_i^k$ and $\breve{Y}_i^k$ will be used as training samples. $\breve{Y}_i^k$is obtained by: $\breve{Y}_i^k$ (l, c) = $Y_i^k$ ($L_y - l + 1$, c), ($l = 1 \ldots L_y$, $c = 1 \ldots C_Y$ ), where $L_Y$ and $C_Y$ are the row number and column number of $Y_i^k$respectively.

Step 2: Use $Z_1$, $X_i^k$s and a palmprint identification method, to calculate the score of Z1 with respect to each class. The score of $Z_1$ with respect to the i th class is denoted by $s_i$ .

Step 3: Use $Z_2$, $Y_i^k$ s and the palmprint identification method used in Step 2 to calculate the score of $Z_2$ with respect to each class. The score of $Z_2$ with respect to the i th class is denoted by $t_i$.

Step 4: $Y_j^k$ ( $j = 1, \ldots, m', m' \leq m$), which have the property of Sim_score($\breve{Y}_j^k$, $X^k$ ) $\geq$ match_threshold, are selected from ($\breve{Y}^k$ as additional training samples, where match_threshold is a threshold. Sim_score(~$\breve{Y}_j^k$, $X^k$) is defined as:

$$\text{Sim-score}\,(Y, X^K) = \sum_{t=1}^{T} (S\widehat{Y}_t,\ X_k)) / T \qquad (1)$$

and

$$S((\widehat{Y}_{t,} X^k) = \max\ (\text{score}\ (\ \widehat{Y}_{t,}\ \widehat{X}_{i_t}^k)),\ i=\{1..m\} \qquad (2)$$

where Y is a palmprint image. $X^k$ are a set of palmprint images from the kth subject and $X_i^K$ is one image from $X^k$. $\widehat{X}_i^k$ and $\widehat{Y}$ are the principal line images of $X_i^K$ and Y, respectively. T is the number of principal lines of the palmprint and t represent the tth principal line. Score(Y, X) is calculated as formula (1) and the Score(Y, X) is set to 0 when it is smaller than sim_threshold, which is empirically set to 0.15.

*Step 5:* Treat $\breve{Y}_j^k$ s obtained in Step 4 as the training samples of $Z_1$. Use the palmprint identification method used in Step 2 to calculate the score of $Z_1$ with respect to each class. The score of the test sample with respect to $\breve{Y}_j^k$ s of the $i$ th class is denoted as $g_i$ .

*Step 6:* The weighted fusion scheme $f_i = w_1 s_i + w_2 t_i + w_3 g_i$, where $0 \leq w_1, w_2 \leq 1$ and $w_3 = 1 - w_1 - w_2$, is used to calculate the score of $Z_1$ with respect to the $i$ th class. If $q = \arg\min f_i$ , then the test sample is recognized as the $q$ th subject

***Matching Score Level Fusion***

In this framework, the final decision making is based on three kinds of information: the left palmprint, the right palmprint and the correlation between the left and right palmprint. The fusion in multimodal biometric systems can be performed at four levels. In the image (sensor) level fusion, different sensors are usually required to capture the image of the same biometric.

Fusion at decision level is too rigid since only abstract identity labels decided by different matchers are available, which contain very limited information about the data to be fused. Fusion at feature level involves the use of the feature set by concatenating several feature vectors to form a large 1D vector. The integration of features at the earlier stage can convey much richer information than other fusion strategies. So feature level fusion is supposed to provide better identification accuracy than fusion at other levels. However, fusion at the feature level is quite difficult to implement because of the incompatibility between multiple kind of data.

Moreover, concatenating different feature vectors also lead to a high computational cost. The advantages of the score level fusion and the weight-sum score level fusion strategy is effective for component classifier combination to improve the performance of biometric identification. The strength of individual matchers can be highlighted by assigning a weight to each matching score. Consequently, the weight-sum matching score level fusion is preferable due to the ease in combining three kinds of matching scores of the proposed method.

The final matching score is generated from three kinds of matching scores. The first and second matching scores are obtained from the left and right palmprint, respectively. The third kind of score is calculated based on the crossing matching between the left and right palmprint. *wi (i* = 1, 2, 3*)*, which denotes the weight assigned to the *i* th matcher, can be adjusted and viewed as the importance of the corresponding matchers.

Differing from the conventional matching score level fusion, the proposed method introduces the crossing matching score to the fusion strategy. When $w3 = 0$, the proposed method is equivalent to the conventional score level fusion. Therefore, the performance of the proposed method will at least be as good as or even better than conventional methods by suitably tuning the weight coefficients.

## IV. PROPOSED METHODOLOGY

Biometrics has long being touted as a powerful tool for solving identification and authentication issues for immigration and customs, forensics, physical and computer security. Multimodal biometric systems are used to increase the performance as well as better security that may not be achievable by using unimodal biometrics. Among various biometrics technologies, palm print identification has received much attention because of its good performance. In this work, left and right palm print of same person is used for improving security. The hybrid fusion method is introduced, which combines the score-level and decision-level fusions, taking advantage of both fusion modes proposed for more accurate personal identification. It adaptively tunes itself between the two levels of fusion, and improves the final performance over the original two levels. The proposed hybrid fusion is simple and effective for combining biometrics. Experiments shows that in different cases, with different matching score distributions, the hybrid fusion method is able to adapt itself for improved performance over the two levels of fusion.

***Decision-level Fusion Framework***

Instead of dealing with the matching scores, the fusion framework works directly on the ROC (receiver operation characteristic). Although the ROC is derived from the matching scores, the problem is still made different: the matching scores are converted into a compact set of operations n points, which convey the distribution information of matching scores in an indirect way. The optimization in the framework only involves those operation points, without reference to the matching scores. Those ROCs could characterize already fused multi-biometrics system.

In this type of fusion method, the decision of person verification is taken based on thresholds obtained by both the modalities. Hence the sample given as input is accepted genuine person only it satisfies both the criteria. Two methods have been used for decision level fusion. (i) Logical Conjunction -'AND' (ii) Logical Disjunction- 'OR

Each biometric system can be characterized by a ROC, i.e., the detection rate $p_d$ ($p_d = 1-\beta$) as a function of false accept rate $\alpha$, denoted by $p_d(\alpha)$. The ROC is obtained by varying the threshold that discriminates the genuine and impostor matching scores, thus producing different detection rate pd and false accept rate$\alpha$. Each point on the ROC, a specific pair of ($\alpha$, pd), is called an operation point, corresponding to a particular threshold t of the matching scores. It show how multiple ROCs can be fused together simply by AND and OR rule for improved performance. When the optimal operation points on ROC are obtained, the thresholds of matching scores are obtained as well.

Suppose it has N independent biometric systems, each characterized by its ROC, pd, i($\alpha_i$), i = 1, ...,N. Besides, the independency assumption makes the formulations much simpler and clearer. If the AND rule is used for fusion, the final performance can be estimated, under the independent assumption, as

$$\alpha = \prod_{i=1}^{N} \alpha_i,\ p_d\ (\alpha) = \prod_{i=1}^{N} p_{d,i}\ (\alpha_i) \quad (3)$$

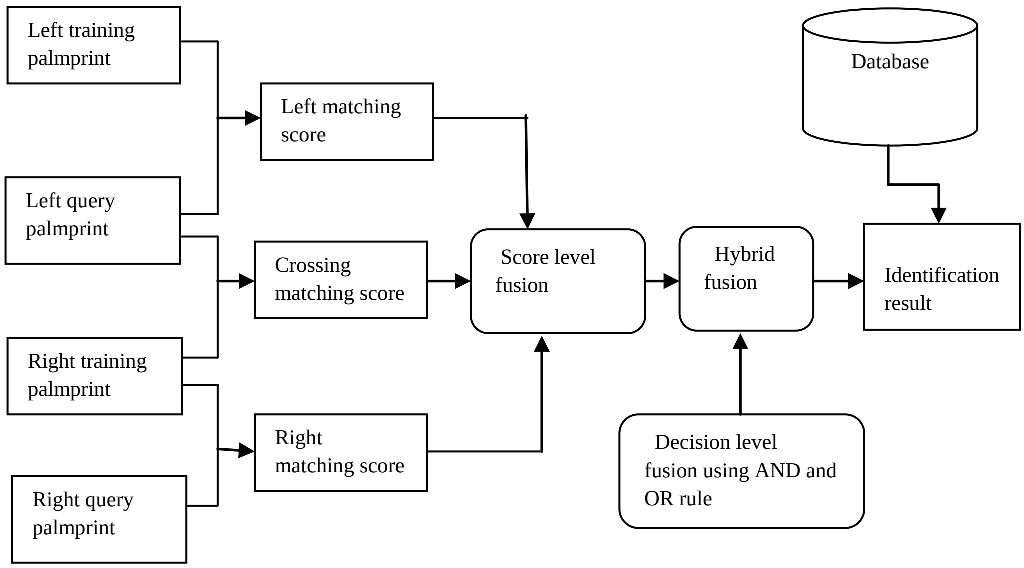


Figure 4: Flow Diagram of the Proposed System

with $\alpha$ the false-accept rate and pd the detection rate of the AND rule fused decision, respectively. In search of the optimal operation points, the fusion framework by AND rule can be formulated as

$$\hat{P}_d(\alpha) = \max_{\alpha_i | \prod_{i=1}^{N} \alpha_i = \alpha} \{\prod_{i=1}^{N} p_{d,i}\ (\alpha_i) \quad (4)$$

which means that the resulting detection rate $\hat{p}_d$ at $\alpha$ is the maximal value of the product of the detection rates at a certain optimal combination of $\alpha_i$ , i = 1, ...,N, which satisfy $\prod_{i=1}^{N} \alpha_i = \alpha$ . In other words, at a prefixed $\alpha$, the optimal operation points of the component ROCs are obtained by optimizing (4). Consequently, the thresholds of component biometric systems can be readily obtained as the ones corresponding to the optimized operation points.

Likewise, if it define the reject rate for the impostors $p_{r,i} = 1 - \alpha_i$, the fusion framework by OR rule can be similarly formulated

$$\hat{p}_r(\beta) = \max_{\beta_i | \prod_{i=1}^{N} \beta_i = \beta} \{ \prod_{i=1}^{N} p_{r,i}(\beta_i)\} \quad (5)$$

It can be easily proved that the optimized detection rate $\hat{p}_d\ (\alpha)$ in (4) is never smaller than any of the component $p_{d,i}$, i = 1, ...,N, at the same $\alpha$, and ˆ$\hat{p}_r\ (\beta)$ in (5) is never smaller than any of the component pr,i, i = 1, ...,N, at the same $\beta$. If a certain classifier cannot help or possibly degrades the overall performance, the optimization will switch it off by tuning its operation points to $\alpha$ = 1, $p_d$ = 1 in case of fusion by AND rule, or $\beta$ = 1, $p_r$ = 1 in case of fusion by OR rule.

In practice, it is in most cases not possible to have the ROC $\hat{p}_d\ (\alpha)$ in analytical form, instead, the ROC has to be estimated from the evaluation data. As a result, $\hat{p}_d\ (\alpha)$ are characterized by a set of discrete operation points rather than a continuous function. The optimization problem formulated in (4) and (5), therefore, has to be solved numerically. In a brute-force way, the optimization could be done by first calculating the pool of operation points, i.e, estimating all the possible combinations by (3), and then select the ones optimal in the Neyman-Pearson sense.

The fusion of three or more ROCs, as proved, can be reduced to iteratively fusing two ROCs. Therefore, the number of possible combinations does not explode rapidly with the number of ROCs, and the complexity of the optimization is kept low. The first ROC is obtained by generating genuine scores as the random variables of Gaussian distribution N(1.5, 1), and impostor scores of N(−1.5, 1), while the second ROC is obtained by generating genuine scores of N(2, 1) and impostor scores of N(−2, 1). The possible operation points after fusion are indicated by dots, while the final optimized points are marked by small squares. It can be observed that both the AND and OR fused ROCs are improved, in the Neyman-Pearson sense, over the two original ROCs.

***Hybrid Fusion***

The motivation for the hybrid fusion is twofold. First, the decision fusion framework using ROCs is very general and can be extended easily. Secondly, by hybrid fusion it hope to take advantage of the score-level and decision-level fusion, and eventually achieve an even more reliable and robust biometric system.

Under the general decision fusion framework, any two or more ROCs can be fused together. A biometric system, which has already been fused, can be easily put into this framework. This enables us to design a new hybrid biometric fusion scheme, combining score-level and decision-level fusion. Suppose the decision-level fusion can be expressed by

$$r_{decision} = D(r_1, ..., r_N) \quad (6)$$

Where $r_1$, ...$r_N$ are the component ROCs to be fused, D is the decision fusion function, and $r_{decision}$ is the resulting ROC. Similarly, suppose the score-level fusion is expressed by

$$r_{score} = S(r_1, ..., r_N) \quad (7)$$

where S is the score fusion function, and $r_{score}$ is the resulting ROC. The hybrid fusion function H is defined as

$$H(r_1, ..., r_N) = D(r_1, ..., r_N, S_1, ..., S_M) \quad (8)$$

Where $S_1$, ..., $S_M$ denotes the ROCs of different score-level fusion methods. In Section 2, we have assumed independency between the component ROCs. In hybrid fusion, however, the assumption is not satisfied, as the inputs in (8), $r_1$, ..., $r_N$ and S($r_1$, ..., $r_N$), are dependent. Strictly speaking, it has to go back to the matching score space, and take into account the joint probabilities of the component matching scores. For example, suppose fusing two classifiers with matching scores $s_1$ and $s_2$, with the genuine score distribution p(s1, s2|$\omega_1$), and the impostor score distribution p(s1, s2|$\omega_0$). The optimization at decision level, in the Neyman-Pearson sense, is

$$\hat{P}_d(\alpha) = \max_{t_1,t_2} \{ \int_{t_1}^{\infty} \int_{2}^{\infty} p(s_1, s_2|\omega_1) d_{s1} d_{s2}) \quad (9)$$

Subject to

$$\int_{t_1}^{\infty} \int_{2}^{\infty} p(s_1, s_2|\omega_0) d_{s1} d_{s2} = \alpha \quad (10)$$

There are methods to solve (9), however, in practice we found that the independency assumption, i.e., solving (4) to obtain the thresholds corresponding to the optimal _i's, is just adequate. The independency assumption might change the estimation of $\hat{P}_d(\alpha)$, but the thresholds t1 and t2 corresponding to its maximal value is often unchanged, or close enough to the real t1 and t2 under the dependent assumption. This is similar to the Naive Bayes problem, which also assumes independency between features, but whose optimality in dependency cases has been acknowledged in a wide range of applications. Actually, observed that in many cases, the results from independency assumption is even better than the results from the dependency solutions. This can be explained by that fact that the optimization problem in (9) has much larger complexity than (4) and therefore more prone to overfit the solutions to the specific training set of matching scores. Solving the hybrid fusion using the ROCs, instead of the matching scores, not only preserves the simplicity of the method, but also makes the solution more robust to the deviations between the training and testing scores. The system summarizes the hybrid fusion method as follows:

1. Given a set of component matching scores, and a set of score-level fusion methods.
2. (Training) Derive individual ROCs from the component matching scores and the score-level

fused matching scores. Fuse all the ROCs under the fusion framework by the AND rule (2) or OR rule (3), and obtain the optimal combination of operation points.

3. Obtain the thresholds corresponding to those optimized operation points.
4. (Testing) Apply the trained thresholds on the component matching scores the score-level fused matching scores, and fuse the decisions by the AND rule or OR rule as the final decision.

## V. EXPERIMENTAL RESULT

The experiments are carried out in Matlab. Matlab is a programming language that can be used for a wide array of numerical and computing applications. The interface follows a language that is designed to look a lot like the notation use in linear algebra. The evaluation of the proposed hybrid fusion approach is compared with that of decision level fusion and score level fusion for determining the efficiency of Accurate Personal Identification .

The left and right palm print of the same person is taken as an input ,which are shown in the figure 5 and figure 6.


Figure 5: Left Palmprint


Figure 6: Right Palmprint

The ROI regions are extracted from both left and right palmprint, which are shown in figure 7 and figure 8.


Figure 7: Left Palmprint ROI Region


Figure 8: Right Palmprint ROI Region

After ROI region extraction, both palmprint are segmented which are represented in figure 7 and figure 8.

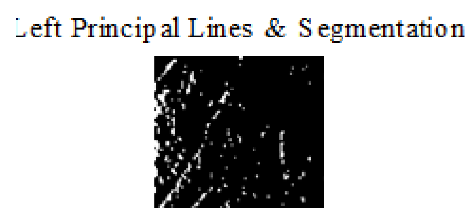


Figure 9: Left Palmprint Segmentation

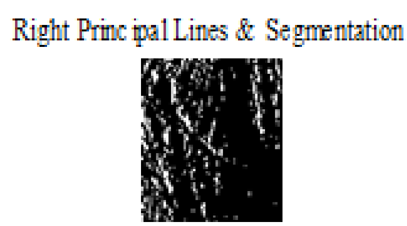


Figure 10: Right Palmprint Segmentation

The first two kinds of scores were, respectively, generated from the left and right palmprint images and can be obtained by palmprint identification method. Then calculate the crossing similarity between the left and right palmprint. Three weight coefficients are assigned to three scores. The weight coefficients $w1$, $w2$ and $w3$ are tuned in step of 0.05. The left palmprint matching scores and right palmprint matching scores should have larger weights than the crossing matching score between the left palmprint and reverse right palmprint.

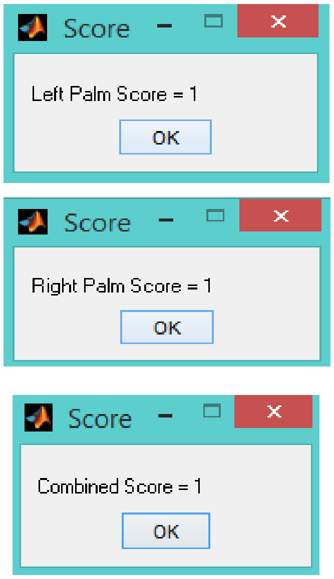


Figure 11: Right Palmprint Segmentation

The combined score value is generated by integrating both left palm score and right palm score , which are shown in figure 11.

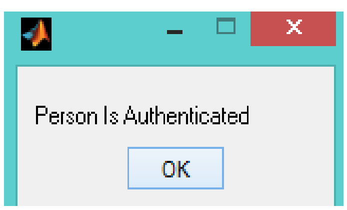


Figure 12: Personal Authentication

The proposed system introduced a hybrid fusion method which combines the score-level and decision-level fusions for personal authentication.

## VI. PERFORMANCE EVALUATION

To evaluate the performance of the proposed approaches, several parameters are used as such as detection rate, false acceptance rate and genuine acceptance rate.

### *False Accept Rate (FAR)*

It defined as the probability of an impostor being accepted as a genuine individual. That is, in a biometric authentication system, the FAR is computed as the rate of number of people is falsely accepted (false people are accepted) over the total number of enrolled people for a predefined threshold.

### *False Reject Rate (FRR)*

It is defined as "the probability of a genuine individual being rejected as an impostor". That is, in a biometric authentication system, the FRR is computed as the rate of number of people is falsely rejected (genuine people are rejected) over the total number of enrolled people for a predefined threshold.

### *False Accept Rate (FAR) Vs False Reject Rate (FRR)*

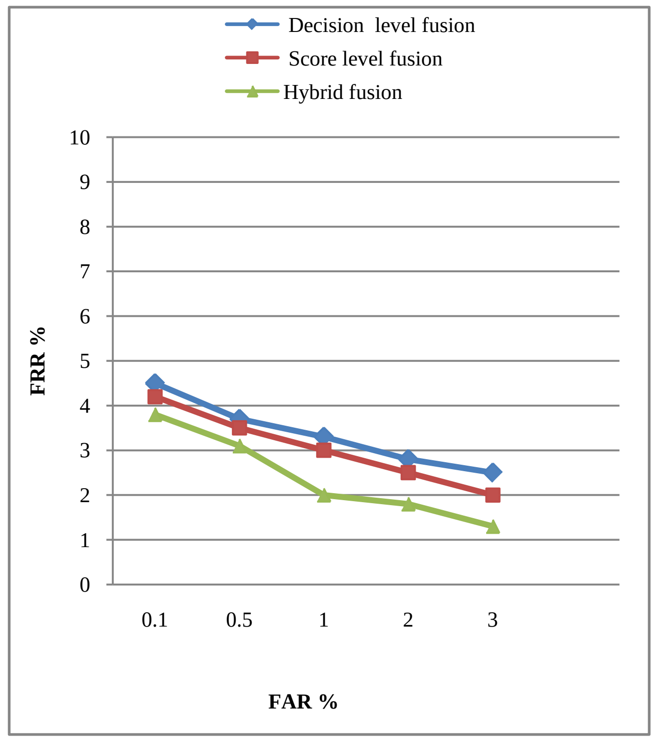


Figure 13: False Reject Rate (FRR) Comparison

The comparison results of the proposed hybrid fusion approach and existing decision level fusion and score level fusion methods in terms of false rejection rate shown in figure 13. In x-axis false acceptance rate is taken and y-axis false rejection rate is taken. From the graph results, it is observed that, the proposed hybrid fusion approach is achieves better result compared with existing methods.

***Detection Rate***

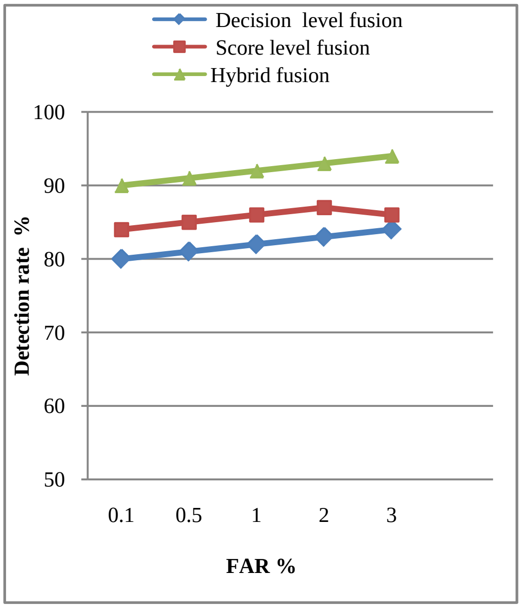


Figure 14: Detection Rate Comparison

Figure 14 compares the detection rate of the biometric system by using proposed hybrid fusion approach and existing decision level fusion and score level fusion. In x-axis false acceptance rate is taken and y-axis detection rate is taken. Hybrid fusion method combines the score-level and decision-level fusions, which taking advantage of both fusion modes. From the graph results, it is observed that, the proposed hybrid fusion approach is achieves better detection compared with existing methods.

***Genuine Acceptance Rate***

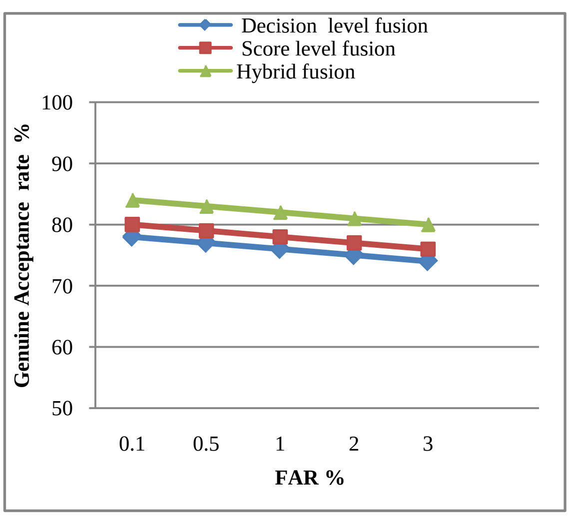


Figure 15: Genuine Acceptance Rate Comparison

The comparison results of the proposed hybrid fusion approach and existing decision level fusion and score level fusion methods in terms of genuine acceptance rate shown in figure 15. In x-axis false acceptance rate is taken and y-axis genuine acceptance rate is taken. The GAR (1–FRR) is the fraction of genuine scores exceeding the threshold. Fig. 17 shows the comparison of proposed system with existing decision level and score level fusion on the basis of genuine acceptance rate and false acceptance rate. It can be easily estimated from the ROC curves that the performance gain is very high as compared to the existing methods.

## VII. Conclusion

The proposed system introduced a hybrid fusion method which combines both decision level and score level fusion methods for achieving accurate personal identification. In this work left and right palmprint of the same subject are correlated and crossing matching score of the left and right palmprint are computed for improving the accuracy of identity identification. Then integrate the left palmprint, right palmprint, and crossing matching of the left and right palmprint for identity identification. Here introduced general fusion framework at decision level, by optimizing the operation points on the ROCs in the Neyman-Pearson sense. Derive individual ROCs from the component matching scores and the score-level fused matching scores. Finally hybrid fusion method is proposed, which combines the score-level fusion and the decision-level fusion. Experiments show that in different cases, with different matching scores distributions, the hybrid fusion method is able to adapt itself for improved performance over the two levels of fusion. More generally speaking, any fusion method could be integrated into this framework and optimized with respect to ROC, with improvements expected in the Neyman-Pearson sense. In future various biometrics such as face, fingerprint is used for improving the identification more.

## REFERENCES

[1] D. Zhang and W. Shu, “Two Novel Characteristic in Palmprint Verification: Datum Point Invariance and Line Feature Matching”, Pattern Recognition, Vol. 32, No. 4, Pp. 691-702, 1999.

[2] Sanjay R. Ganorkar and Ashok A. Ghatol, “Iris Recognition:An Emerging Biometric Technology”, International Conference on Signal Processing, Robotics and Automation, Greece, Pp.91-96, 2007.

[3] A. Ross, S. Dass and A. K. Jain, “A deformable model for fingerprint matching”, Journal of Pattern Recognition, Elsevier, Vol. 38, No. 1, Pp. 95-103, 2005.

[4] A.K. Jain, A. Ross and S. Pankanti, “Biometric: A Tool for Information Security”, IEEE Trans. Information Forensics and Security, Vol. 1, No. 2, Pp. 125–144, 2006.

[5] M.A. Dabbah, W.L. Woo and S.S. Dlay, “Secure Authentication for Face Recognition”, Proc. of IEEE Symposium on Computational Intelligence in Image and Signal Processing, Pp. 121–126, 2007.

[6] A.K. Jain, A. Ross and S. Prabhakar, “An introduction to biometric recognition”, IEEE Trans. Circuits Syst.Video Technology, Special Issue Image and Video-Based Biometric, Vol. 14, No. 1, Pp. 4–20, 2004.

[7] A.K. Jain, A. Ross and S., Pankanti, “Biometrics: A Tool for Information Security”, IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, Pp 125–144, 2006.

[8] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain, “FVC2002: Fingerprint Verification Competition”, Proc. International Conference on Pattern Recognition (ICPR), Pp. 744-747, 2002.

[9] J.L. Wayman, “Fundamentals of Biometric Authentication Technologies”,International Journal of Image and Graphics, Vol.1, No.1, Pp. 93-113, 2001.

[10] V. Matyas and Z. Riha, “Toward reliable user authentication through biometrics”, IEEE Security & Privacy Magazine, Vol. 1, No.3, 2003.

[11] N.K. Ratha, J.H. Connell and R.M. Bolle, “Enhancing security and privacy in biometrics-based authentication system”, IBM Systems Journal, Vol. 40, No. 3, Pp. 614-634, 2001.

[12] Gyaourova and A. Ross, “Index codes for multi biometric pattern retrieval”, IEEE Trans. Inf. Forensics Security, Vol. 7, No. 2, Pp. 518–529, 2012.

[13] J. Dai, J. Feng and J. Zhou, “Robust and Efficient Ridge-Based Palmprint Matching”, IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol.34, No. 8, Pp. 0162-8828, 2012.

[14] S. Ben-Yacoub, Y. Abdeljaoued and E. Mayoraz, “Fusion of face and speech data for person identity verification. Neural Networks”, IEEE Transactions on neural networks, Vol. 10, No. 5, Pp. 1065-1074, 1999.

[15] R. Choraś, “Multimodal Biometric Personal Authentication Integrating Iris and Retina Images”, Image Processing and Communications Challenges, Vol. 2, Pp. 121-131, 2010.

[16] X. Pan and Q.Q. Ruan, “Palmprint recognition using Gabor feature-based (2D)2 PCA”, Neurocomputing, Vol. 71, Pp. 3032–3036, 2008.

[17] X. Pan and Q.Q. Ruan, “Palmprint recognition using Gabor-based local invariant features”, Neuro computing, Vol. 72, No. 7–9, Pp. 2040– 2045, 2009.

[18] X. Wang, L. Lei and M.Z. Wang, “Palmprint verification based on 2D-Gabor wavelet and pulse-coupled neural network”, Knowledge-Based Systems, Vol. 27, Pp. 451–455, 2012.

[19] K. Adams, Z. David, K. Mohamed, “A survey of palmprint recognition”, Pattern Recognition, Vol.42, Pp.1408-1418, 2009.

[20] S.L. Happy, A. George, and A. Routray, “A real time facial expression classification system using Local Binary Patterns”, 2012 4th International Conference on Intelligent Human Computer Interaction (IHCI),2012.

[21] G.S. Badrinath and P. Gupta, “Stock well transform based palm-print recognition”, Elsevier, Pp. 4267–4281, 2011.

[22] C.C. Han, H. L. Cheng , C.L. Lin and K.C. Fan, “ Personal authentication using palm-print features”, Elsevier, Pp. 371–381, 2003.

[23] S. Ibrahim, H. Jaafar and D.A. Ramli, “Robust Palm Print Verification System Based on Evolution of Kernel Principal Component Analysis”, IEEE International Conference on Control System, Pp. 28-30, 2014.

[24] S. Biradar, “Personal Identification Using Palmprint Biometrics Based on Principal Line Approach”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 2, No. 7, 2013.

[25] H. Imtiaz, and S.A. Fattah, “A wavelet-based dominant feature extraction algorithm for palm-print recognition”, Digital Signal Processing, Vol. 23, No. 1, Pp.244-258, 2013.