Abstract—True identity of an individual is the main advantage of a biometric system. Palmprint provides more distinct and distinguishing features for identifying a person. Different types of palmprint image exhibits different features. Feature extraction method depends on the palmprint image used. High resolution palmprint images which are mainly employed in high security forensic applications concentrates on minute features such as ridges, minutiae and pores. Images captured by forensic experts from the crime scene usually called as latent images are almost partial. The use of minutia for authenticating these images is a promising and challenging approach. It is very difficult and sometimes even impossible to replicate minutia points. Novel strategies need to be developed for an efficient palmprint authenticating system to improve its performance for large scale applications. This paper presents a high resolution palmprint authenticating system based on minutiae feature. In the proposed method, pattern descriptors are employed to extract the minutia points. This is a novel approach designed specifically to process high resolution palmprint image.

Index terms—High resolution Palmprint, feature extraction, minutiae, Pattern descriptors.

I. INTRODUCTION

Today’s security system concentrates on identifying an individual aptly. The main benefit provided by the biometric system is that it authenticates an individually automatically. Nowadays, palmprint has emerged into the research field due to its abundant distinct and reliable features such as principal lines, wrinkles and ridge-based features. Based on the resolution of the image and features used palmprint authenticating systems are categorized into two groups [1]. Features such are principal lines and wrinkles alone could be extracted from low resolution images (~100 dpi) and ridge-based features in addition to principal lines and wrinkles can be extracted from the high resolution images (~500 dpi). Palmprint ridges are 18% larger in width compared with fingerprint [2]. Ridges features are further classified as ridge orientation, ridge density, ridge length, count, minutiae points namely termination, bifurcation and pores which are very minute. Fig. 1 summarizes the types of image and the available features of palmprint.
High resolution images are mostly offline images. These images are used by the forensic experts to suspect a victim. Offline images which are inked images are converted into a digital image by the use of digital scanner. Latent images are images captured from the crime scene which are used in high security forensic applications. Latent prints identified from knife hilts, gun grips, steering wheels and window panes are mostly from palms, not fingers [2]. These images are almost partial and thus a challenging one for a biometric system. Fig. 2 shows a part of a palmprint with ridge-based features.

![Fig. 2. Ridge-based Features](image)

The paper is organized as follows: Section II summarizes the literature survey. Section III describes the proposed novel pattern descriptors for extracting minutia features from the palmprint. The details of the database used for the experiment and results are presented in section IV. Section V concludes the work done.

II. LITERATURE SURVEY

Line-based features are not as reliable as ridge-based features. Ridge features include ridge orientation, ridge density, ridge end points and ridge bifurcations termed as minutiae points, pore features etc. These ridge features can be obtained only from the palmprint images whose resolution is at least 500 dpi. Moreover, 500 dpi is a standard resolution used for identifying a person. Identifying a person using ridge-based features is being accepted in the court of law nowadays [3]. The features used in the palmprint recognition and the accuracy that can be obtained are summarized in Table 1.

<table>
<thead>
<tr>
<th>Features</th>
<th>Image Resolution</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lines</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Ridge</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Minutiae</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Pore</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Minutiae points are the ridge endings or bifurcation of the ridges. A full palmprint contains about 1000 minutiae points [4]. Algorithms of fingerprint authenticating system can be used for palmprint authenticating system. But the presence of creases in the palm, introduces false minutiae. A large number of false minutiae produced around these creases should not be considered while matching and must be removed before matching. The literature for minutia-based palmprint authenticating system is very sparse till now. Table 2 summarizes the methods used to extract minutiae points and the performance analysis.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Technique Used</th>
<th>Performance analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>In [1]</td>
<td>Minutia Triplet in fusion with multiple features</td>
<td>-</td>
</tr>
<tr>
<td>In [2]</td>
<td>Minutia Code</td>
<td>Partial to full matching : GAR = 78.7 %</td>
</tr>
<tr>
<td>In [4]</td>
<td>Minutiae Clustering</td>
<td>Latent to full matching : GAR = 69%</td>
</tr>
<tr>
<td>In [5]</td>
<td>MCC descriptors, Local to Global Matching</td>
<td>EER : 0.01%</td>
</tr>
<tr>
<td>In [6]</td>
<td>Minutia Triplet, hierarchical matching</td>
<td>Reduced searching time</td>
</tr>
<tr>
<td>In [7]</td>
<td>Radial Triangulation</td>
<td>Latent to full matching : GAR = 69%</td>
</tr>
<tr>
<td>In [8]</td>
<td>CN Method</td>
<td>-</td>
</tr>
<tr>
<td>In Proposed</td>
<td>CN Method</td>
<td>Full to full matching : GAR = 90.89%</td>
</tr>
<tr>
<td>In Proposed</td>
<td>Pattern Descriptors Method</td>
<td>Partial to Full Matching : GAR = 83.67%</td>
</tr>
</tbody>
</table>
System developed for commercial applications support only a full to full palmprint matching. For a forensic application, matching is based on a partial or latent to full palmprint. Partial images are images cropped from a full palmprint. The principal lines present in the palmprint divides the palm into three different regions namely thenar, hypothenar and interdigital as shown in fig. 3. If a latent or a partial image is from the thenar region, authentication is a challenging one because this region consists of dense thin creases. Algorithms which are robust and efficient are to be improved and developed to meet the requirements of the palmprint authenticating systems employed in high security applications.

III. MINUTIA FEATURE EXTRACTION METHOD

The Core characteristic of a biometric system is its feature extraction method. Feature extraction is the process of converting the input image into a data or signal that is used to compare with the template stored in the database. Here, the data is transformed to a reduced feature represented in form of feature vector.

The proposed method includes the following steps.

1. The input image is accepted
2. The input image is converted from the jpg format to uncompressed png format
3. During preprocessing, thinning image is obtained
4. From the thinned image minutia features are extracted as described below
   4.1 Patterns of size 3 x 3 are defined to extract minutia points
   4.2 Sliding is being done with these non-overlapping 3 x 3 patterns
   4.3 Convolution process is defined as

   \[ Z(t) = x(t) * y(t) \]  \hspace{1cm} (1)

   where \( x(t) \) is the 3 x 3 sub-image and \( y(t) \) is 3 x 3 patterns as shown below

   **Bifurcation Patterns (\( \times \) denotes bifurcation point)**

   ![Bifurcation Patterns](image)

   **Termination Patterns (\( + \) denotes termination point)**

   ![Termination Patterns](image)
4.4 Convolution process is carried out in the 3 x 3 sub-image as

\[ Z(t) = \sum_{i=1}^{r} \sum_{j=1}^{c} [x(i,j)] * y(t) \]  \hspace{1cm} (2)

where \( i, j \) are rows and columns respectively, \( x \) the sub-image and \( y(t) \) the patterns.

After this process, termination and bifurcation point are identified.

5. Existence of the false minutia points are removed by using the following method

\[ Z = b + t \]  \hspace{1cm} (3)

where \( b \) are bifurcation points and \( t \) are termination points.

5.1 For each and every point, the calculation is as follows

\[ Z(i,j) = \sum_{i=1}^{r} \sum_{j=1}^{c} [b(i,j) + e(i,j)] \]  \hspace{1cm} (4)

where \( r \) and \( c \) denotes the rows and columns in the sub-image.

5.2 11 x 11 non-overlapping sub-image is considered for the above process.

5.3 Unwanted minutia points are removed if the following criteria occurs

\[ \times \text{ denotes Bifurcation} \quad \quad \quad \quad \quad \quad \quad \text{Type 3 : 1 Termination and more than 1 Bifurcation} \]

\[ + \text{ denotes Termination} \quad \quad \quad \quad \quad \quad \quad \text{Type 4 : More than one Termination} \]

Type 1 : Termination and Bifurcation

\[ \times \]

\[ + \]

Type 2 : 1 Bifurcation and more than one termination

\[ \times \]

\[ + + \]

Type 5 : More than one Bifurcation

\[ \times \]

\[ + \]

IV. EXPERIMENTAL RESULTS

Matching process finds or confirms whether the person has previously enrolled in the system or not. Here, the distinctness between the gallery and the query palmprint is found out. If, the system produces a small intra-class variance and a large inter-class variance then it is a perfect match.

Depending upon the size of the input palmprint image, matching is performed which may fall among the following three categories namely full-to-full palmprint matching, latent-to-full palmprint matching and partial-to-full palmprint matching [4]. Generally, Full-to-full palmprint matching is not used in forensic applications since the images captured from crime scenes are partial. Thus, performing partial-to-full palmprint matching is necessary in such situations.

For the experiment the publicly available high resolution THUPALMLAB database is used. This database contains 1,280 palmprint images from 80 subject (two palms per person and eight impressions per palm) using a commercial palmprint scanner of Hisign. The image size is 2040 x 2040 pixels, having 256 gray levels and the image resolution is 500 dpi. This database is available at http://ivg.au.tsinghua.edu.cn. Fig. 4 shows the input image and the portion the palmprint after extracting minutia point.
Fig. 4. Input image and portion of it showing the extracted minutia points

Usually, the performance analysis is performed by computing False Acceptance Rate (FAR), False Rejection Rate (FRR) and Genuine Acceptance Rate (GAR). False acceptance is a situation where a person who has not registered gains access to a biometric protected system. This happens if matching of biometric input with the template in the database is incorrect. FAR is the probability where an imposter is accepted. False rejection is where a user who has enrolled does not gain access to a system which is biometrically protected i.e., a situation where the system fails to match the input with the template stored in database. FRR is the probability where a genuine user is rejected. The GAR is computed as the ratio of the number of genuine matches found by the system to the total number of matches actually performed by the biometric system. GAR value gives the strength of a biometric system.

Receiver Operating Characteristics (ROC) curve which summarizes the performance of matching systems is universally accepted. This curve plots the rate of imposter attempts accepted on the x-axis, against the corresponding rate of genuine attempts accepted on the y-axis. Performance comparison of different systems under similar conditions or a single system under different conditions is shown in this ROC curve. Here, ROC curve in fig. 5 illustrates the performance obtained from ridge endings, bifurcation points and the combination of both the features. Fig. 6 shows the ROC curve illustrating the performance of the proposed pattern descriptors method with various methods for THUPALMLAB database.

Fig. 5. ROC curve illustrating the performance of palmprint authentication system using termination points, bifurcation points and the combination of these two minutiae features for pattern descriptor method
Fig. 6. ROC curve illustrating the performance of palmprint authentication system using minutiae feature for various methods for THUPALMLAB Database

V. CONCLUSION AND FUTURE WORK

The overall performance of the palmprint recognition system using principal line and wrinkles alone is less. This paper is an attempt to identify a person based on minutiae feature present in palm. Yet to our knowledge, pattern descriptors have not been used to extract minutiae feature for authenticating palmprint. Hence by using this method it has been proved that the performance of the system is improved compared with the existing system. But still, robust partial palmprint feature extraction algorithms are required ha has to be developed. Distortions are very common in the palmprint images of the same person captured at different situations. Still there are many challenges which are to be solved for large scale applications. For achieving the state-of-art performance minutia feature in fusion with ridge and pore features can be tried out to further improve the overall performance of the palmprint authentication systems used in high security application.

References
