CHAPTER 4
EXTRACTION OF NEW FEATURE IN EAR USING HOUGH TRANSFORMS

Authentication plays a vital role in accessing the confidential information and resources. As seen in the previous chapter, ear authentication was carried out using feature extraction techniques. Though the sample images considered were free from occlusions and rotation invariant, the accuracy of the method was not very high and the number of images considered was less. Hence, it was decided to carry out ear authentication using Hough transform which is one of the techniques used to extract the features of ear images under different poses and illuminations. The proposed system uses Hough transform to extract the new feature in the ear based on Hough lines in such a way that it considers the images of different poses and illumination. This thesis, therefore, aims at developing a modular, robust, biometric authentication system which utilizes an ear profile, by the use of Hough Transform.

4.1 FEATURE EXTRACTION USING HOUGH TRANSFORM

The proposed technique authenticates a person using the ear as a biometric by exploiting its inherent geometric and structural details and is rotation and scale invariant. The increasing variety of biometrics applications in everyday identification and authorization problems urges the development of easily applicable methods. The ear is largely a planar shape and 3D must penetrate the intricate inner ear, which restricts deployment potential. In the case of 2D recognition, detecting ears from cropped side face 2D images is a challenging problem due to the fact that ear images can vary in appearance under different viewing and illumination conditions [67]. A suitable way of finding the features of ear images under various environmental conditions by the use of the Hough transform is proposed which is
tolerant to rotation and illumination variation. This ear authentication system comprises of three stages namely:

Stage I: Pre-processing,

Stage II: Localization and Feature extraction using Hough Transform

Stage III: Matching

In the preprocessing stage, the ear image is normalized and standardized to a common format. Then the feature extraction algorithm is applied on the ear image. Originally the edges belonging to ear are curved [89]. But the Hough Transform (HT) breaks every edge of the outer ear into a set of line segments called Hough Lines. This makes it more compact for further processing. The distance score is calculated for each longest Hough line. Each user is assigned a secret code for authentication. The distance scores generated and the secret codes are combined to form a feature vector for matching. The block diagram of the proposed ear authentication system is shown in the Figure 4.1. The authentication proceeds in two phases: Enrolment phase and Verification phase.

Verification Phase

Enrolment Phase

Figure 4.1 Block Diagram of the ear authentication system
4.1.1 Enrolment Phase

Enrolment (or registration) in an automatic biometric system is the process of detecting and isolating the area of interest [64]. The enrolment data record comprises of one or multiple biometric references and other non-biometric data such as a unique password. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrolment. It consists of the two steps: Pre-processing and Localization using Hough transform.

4.1.2 Verification Phase

First, in verification (or authentication) mode, the system performs a one-to-one comparison of a captured ear image with a specific template stored in a biometric database in order to verify that the individual is the person they claim to be.

Two steps are involved in the verification of a person: - feature extraction and matching. In the first step, the images are subjected to feature extraction to produce a feature vector. The feature vectors of enrolled image and query image are then matched. If the distance is less than a threshold, the person is authenticated. The Equal Error Rate (EER) is taken as the threshold value because False Acceptance Rate (FAR) is equal to False Rejection Rate (FRR) at EER. Error rates, specified by thresholds on Receiver Operating Characteristics (ROC), give some direction in choosing the operating point of biometric system. The EER actually defines a fixed point on the ROC for a given database and matching function.

4.2 ENROLMENT PROCESS

A total of 104 ear images of 26 individuals are enrolled, with each individual having 4 images captured under varying environmental conditions. One of the 4 images is the training image. The system is tested against the other three. The ear images are used from the IIT Delhi Database.
4.2.1 Pre-Processing

In this approach the ear part was manually cropped from the side face image and the portions of the image which do not constitute the ear were colored black leaving only the ear. But due to the noise in the image, noisy edges may be detected only partially. Low pass filtering, otherwise known as "smoothing", was employed to remove high spatial frequency noise from a digital image is performed using the Wiener filter. The median filter was applied to restore blurred edges and to remove the strong vertical edges which are part of image borders. They were created when the region containing the ear is cropped from the side face image. The edges of ear image are represented in white and the remaining area is made black by image binarization. Edge detection is performed using the Sobel operator [90]. The Sobel operator is Sobel filter within edge detection algorithm to emphasize the edges and transitions in ear images as shown in Figure 4.2.

![Figure 4.2 Edge detected image](image-url)

It can be seen that from Figure 4.2, that, the Sobel operator works best for the image as the edges were preserved and were not approximated to form a smooth curve. The outliers were removed properly. The edge detector detected both horizontal and vertical edges in the ear image.
4.2.2 Localization and Feature Extraction using Hough Transform

This approach proposes the use of the Hough Transform (HT), which can extract shapes with properties tolerant of noise and occlusion, to find the elliptical shape of the ears in 2D head-profile images. The feature extraction stage prepares an acquired sample for matching and authentication by separating the object of interest from the background. It is an important step for any automatic biometric authentication system.

The algorithm finds the elliptical shapes in cropped 2D side face images by using a Hough transform to gather votes for the region. Voting is a general technique where the features vote for all models that are compatible with it. Hough Transform is a voting technique that can be used to record vote for each possible line on which each edge point lies and look for lines that get many votes. The regions having maximum votes are plotted as edges. Such curved edges are fitted to straight lines forming a connected edge map. The problem, therefore, is decomposed into several constrained sub problems i.e. Hough lines. The smaller edges which do not form the boundary are removed leaving only the location of the outer boundary of the ear. Thus the problem of detecting collinear points can be converted to the problem of finding concurrent curves [63].

4.2.3 Ear Localization and Approximation of Edges using Line Segments

Ear localization first builds the edge map, and uses it in finding the collinear points in the map for ear localization purpose. Hough transform is performed on an edge detected ear image. Each white pixel on the edge detected binary image is represented as a coordinate pair in parameter space \((ρ,θ)\). For each edge point \((x_i,y_i)\), the value of \(ρ\) is calculated as 
\[ x_i \cos θ + y_i \cos θ = ρ, ρ ∈ [-90, +90] \]. The \(ρ-θ\) plane is partitioned into cells. The spacing between each such cell along the \(ρ\) axis is 1 degree and 1 degree along \(θ\) axis. A 2D array called accumulator \(A(ρ,θ)\) is used to store the value of \(ρ\) and \(θ\) for all edge points in a cell. A voting procedure is then carried out in the parameter
space on A. For each edge point the accumulator is incremented as given in Equation (4.1)

\[ A(\rho, \theta) = A(\rho, \theta) + 1 \quad \text{(4.1)} \]

At the end of this procedure, \( A(\rho, \theta) = P \), means there are P points in this edge. A graph is plotted for the values of the accumulator bin, \( A(\rho, \theta) \).

The Figure 4.3 shows the plot for the values of \( A \). These are plotted for the lines with rotation -90 to +90 degrees, since ear image is elliptic in nature. The point of intersection of these sinusoidal curves represents point of intersection of the lines in coordinate space. But they are mostly parallel corresponding to non-intersecting lines on the ear boundary. The white boxes in the Figure 4.3 show the peaks of the curves, which are the maxima of the curves. Threshold of 50% was applied to the accumulator and the values above the threshold was considered as peaks and retained.

![Figure 4.3 Sinusoidal curves in parametric form](image-url)
These peaks correspond to the strong lines in the image. The Hough Transform maps the curved features of the ear onto straight lines. This makes it accurate in detecting connected components in outer ear images which have been captured under different environmental conditions like illumination or noise. Due to such variations curved edges are often only partially detected as broken edges. Hough Transform detects the contours of such outer ear images effectively. The curved edges of the outer ear are mapped onto straight lines called Hough Line. The length of the longest Hough Line, called max-line, is considered as the feature which is used for matching.

4.3 VERIFICATION PROCESS

During the verification process, the feature vector was extracted as explained in the enrolment process. It undergoes two phases namely 1. Extraction of Distance Score and 2. Matching. The straight lines extracted as discussed in the section 4.2.3 are fitted to the curvature of the outer ear forming an edge map as shown in Figure 4.4. The edges which are linear (or almost linear) need only two points for their representation after line segment fitting. In this manner the curved edges are broken down into a set of straight lines called Hough Lines. The Hough Lines are plotted on the binary ear image. The lines are green in color. Their end points are depicted in red and yellow. Let the set of Hough lines of an image be $\chi$.

4.3.1 Extraction of Distance Score

The query feature has to be compared with that of the enrolled feature. The Euclidean distance between end points of each Hough Line segment in $\chi$ is calculated. Let the distances so obtained are $\gamma$. The distance score is defined as $\beta = \max (\gamma)$.

The line is highlighted in blue is the longest line extracted from the Hough lines as shown in Figure 4.4.
The above procedure was performed for all the test images in the gray scale format and the result set stored for further matching and comparison.

4.3.2 Matching

First, in matching mode the system performs a one-to-one comparison of captured ear image with that of the claimed identity template stored in an ear image database in order to verify the individual is the person they claim to be. If the length of the Hough line of both the query image and the enrolled image is same, then the person is authenticated. If the difference between the enrolled image and query image is less than the threshold then the person is authenticated. Initially the varying thresholds were applied for calculating the error rates. From that, the EER was taken as the threshold value to authenticate the person.

4.3.2.1 Ear image database

It contains the ear images of different people taken from the IIT Delhi database. Images of 26 subjects having a resolution of 204x272 are taken with each subject having 4 images of varying rotation, intensity or illumination and stored.
4.3.2.2 Secret code

Both the images are placed in separate folders with their names as a unique secret code assigned to every individual. Images of the same subject have the same code. One of the images is used as sample input in the enrolment process and all the other images used in the verification process.

4.3.2.3 Security & two part matching

Firstly the secret code is submitted at the time of comparison. Any user cannot access the system without the knowledge of the secret code. This prevents fake login attempts.

Let the secret code for a particular subject be $\beta_1$. Let the distance score for the ear image be $\beta_2$. The distance score and the secret code form a feature vector $\alpha = [\beta_1, \beta_2]$ where $\alpha$ is the feature vector of the query image.

Let the feature vector of the reference image be $\alpha' = [\beta'_1, \beta'_2]$ where the secret code is $\beta'_1$ and $\beta'_2$ is the corresponding distance score. Now the reference image submitted by the user during the enrollment phase, having secret code $\beta'_1$ is fetched.

The distance $D$ between the two feature vectors is calculated as the Manhattan distance between the two distance scores, $\beta_2$ and $\beta'_2$ as

$$D = |\beta_2 - \beta'_2| \text{ where } \beta_1 = \beta'_1$$

The distance $D$ is calculated as the distance between the max-lines provided their secret codes $\beta_1$ and $\beta_1'$ are identical, i.e.; the distance is found between the enrolled image of a particular user and the test image of a user who claims to be a legitimate user.
4.3.2.4 Authentication

If D is less than a threshold then a match is found. A threshold of 70% is used. It is the point where FAR is equal to FRR. If the distance D between two images is less than 70%, then the images are said to be matched. The person is verified to be who he/she claims to be. The results of the matching procedure are stored for further analysis.

4.4 PERFORMANCE MEASURE OF THE SYSTEM

The system performance is calculated using the parameter accuracy. Ideal system indicates that the accuracy of the system is 100%. i.e. the system is error free with FAR and FRR equal to ‘0’. It means that no non-genuine person is falsely accepted as correct person or no genuine person is falsely rejected as imposter. In order to analyze the system performance for varying thresholds FAR and FRR are calculated. The EER is found from FRR versus FAR. The EER is kept as the threshold to authenticate the person.

4.4.1 FAR, FRR and EER Analysis

The technique is tested against the IIT Delhi Ear database, with 26 enrolled users. Each subject has 4 images taken under different angles and illumination. Total of 104 images are enrolled. One image per subject is used as the training image and the test dataset contains three images per subject. The system prompts for the secret code and then the ear image. The Figure 4.5 shows the request for the secret code and Figure 4.6 shows the submission of the corresponding ear image. Now if the query image matches with the secret code, then the corresponding enrolled image is verified based on the distance score using Manhattan distance method. The different values of threshold were taken and the corresponding False Acceptance Rate (FAR) and False Rejection Rate (FRR) calculated. The FAR and FRR are plotted for varying thresholds from 40% to 85% in and recorded as shown in the Table 4.1.
The secret code assigned during the enrolment phase is submitted by the user. In Figure 4.6, the user submits the image for authentication.

Figure 4.6 User then submits a query image
Table 4.1 FAR and FRR on Different Thresholds

<table>
<thead>
<tr>
<th>No.</th>
<th>Threshold in %</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>40</td>
<td>0</td>
<td>0.070</td>
</tr>
<tr>
<td>2</td>
<td>45</td>
<td>0</td>
<td>0.070</td>
</tr>
<tr>
<td>3</td>
<td>50</td>
<td>0</td>
<td>0.060</td>
</tr>
<tr>
<td>4</td>
<td>55</td>
<td>0</td>
<td>0.060</td>
</tr>
<tr>
<td>5</td>
<td>60</td>
<td>0</td>
<td>0.030</td>
</tr>
<tr>
<td>6</td>
<td>65</td>
<td>0</td>
<td>0.030</td>
</tr>
<tr>
<td>7</td>
<td>70</td>
<td>0</td>
<td>0.020</td>
</tr>
<tr>
<td>8</td>
<td>75</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>80</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>85</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Avg FAR=0.1  Avg FRR=3.4

From the plot FAR Vs threshold in Figure 4.7, it can be seen that for a threshold value from 40% to 70%, the FAR is 0, which depicts that system performed efficiently and rejected all the impostor images. FAR is optimum at 70%.

Figure 4.7 FAR Vs Threshold
The FRR declines rapidly with the increase in threshold from 40% to 75% as shown in Figure 4.8.

![FRR vs Threshold](image)

**Figure 4.8 FRRVsThreshold**

The system performs efficiently from a threshold of 75% to 80% by rejecting all the impostor images. The Equal Error Rate (EER) is found to be 2% from Figure 4.9.

![Equal Error Rate (EER)](image)

**Figure 4.9 Equal Error Rate (EER)**
The accuracy of the system is 98.26% which is calculated as shown in Equation (4.2)

\[
\text{Accuracy} = 100 - \left(\frac{\text{FAR} + \text{FRR}}{2}\right) = 100 - \left(\frac{0.1 + 3.4}{2}\right) = 98.26\%
\]

(4.2)

The FAR was observed to be ‘0’ for the threshold of 40% to 70%, after that FAR increased gradually till 75%, after which FAR went to one, showing that the system correctly rejected the imposters till 70% of threshold and after 75% of threshold the system falsely accepted all the imposters. Mainly the system depends upon the threshold value. For the system to behave as an authentication system, the threshold has to be chosen as 70%.

The FRR of the system was ‘0’ from the threshold of 75%. This showed that from this threshold the system did not reject any genuine users. But till 75% of threshold, the system rejected the genuine users. From 40% of threshold, the system gradually reduced from 0.07 rate, i.e. 99.93% it behaved correctly however, 0.07% did not behave well. The equal error was calculated by plotting FAR versus FRR, the point where both the curves met gave the EER of the system. For the system to behave as a proper authentication system, the EER is taken as the optimal threshold.

4.4.2 Authentication of the System

The authentication of the system is identifying the claimed identity to be correct and not accepting the non-genuine users at any cost. The proposed system performed well for a threshold of 70%. Due to an average error rate of 0.1 and 3.4, the accuracy of the system was 98.26%. Till 70% of the threshold, FAR was 0 and average FRR was 0.049, so the accuracy of the system is 99.95%.
If the ear images match, the system displays a message ‘Match’ as shown in Figure 4.10. If they do not match as in Figure 4.11, the system displays a message ‘Not match’.

The authentication system has a good FAR until the threshold of 70%. The FAR is maintained at zero till 70% threshold. The system behaves as a perfect
system which rejects all impostors. Some genuine users are also classified as impostors. This is better because, the system does not authenticate and grant access to false users in any case. Some genuine users rejected do not pose much of a threat than granting access to fake users. The FRR has a maximum value of 0.07 and declines rapidly. It can be seen that FRR is initially 0.07% and declines rapidly; it is maintained at 0 after a threshold of 75%.

![Graph of FAR vs FRR](image)

**Figure 4.12 FAR vs FRR**

The graph of FAR versus FRR is plotted as shown in Figure 4.12 above, for threshold of 40% to 85%. The curve of this system is on the axes until a threshold of 70%. It thereby gives enhanced output due to the scale, rotation and illumination invariance of the algorithm until this threshold.

**Table 4.2 Comparison of accuracy**

<table>
<thead>
<tr>
<th>Method used</th>
<th>No of Test Images</th>
<th>% Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected edge based</td>
<td>490</td>
<td>95.88</td>
</tr>
<tr>
<td>Reduced Hough Transform</td>
<td>252</td>
<td>91</td>
</tr>
<tr>
<td>Outer Helix curve based [7]</td>
<td>700</td>
<td>93</td>
</tr>
<tr>
<td>Proposed Method (Hough Transform)</td>
<td>100</td>
<td>98.26</td>
</tr>
</tbody>
</table>
The Table 4.2 above compares the accuracy of the various existing algorithms. Number test images considered in all the exiting method is more and the classifiers are different. The proposed system accuracy is 98.26%, but the result obtained is only by considering 100 samples of few occluded images and of different poses and rotation. The effective system has to be devised with more number of images and of occlusions.

4.5 SUMMARY

This work implemented an efficient technique for automatic ear authentication using structural details of the ear. The technique detected the contours of the outer ear. The ear was extracted from the side face image by the use of Hough transform to build an edge map. It was able to authenticate persons when ear images were captured with different rotations, angles and illumination efficiently based on the edge map and a secret code assigned to each user. The use of the secret code increased the security of the system as it prevented circumvention. The proposed technique was tested on a database containing 25 subjects with four images each and achieved an accuracy of 98.26%. The FAR was maintained at 0 until a threshold of 70%. The FRR is initially 0.07% and declined rapidly with the increase in threshold. It was maintained at 0 after a threshold of 75%. Hence, a suitable trade-off between FAR and FRR was achieved at 70 % threshold. The system may classify some genuine users as impostors but does not grant access to fake users thereby securing the system. This proposed system has considered only few images with occlusions.