Design of Biometric Authentication System using Three Basic Human Traits

Palvi Sharma¹, Manit Kapoor², Dr. Naveen Dhillon³

¹M-TECH Student, R.I.E.T Phagwara
²Assistant Professor, R.I.E.T Phagwara
³Professor, RIET Phagwara

Abstract: Today's single biometrics feature is not sufficient to provide secure authentication. Most of the multi-modal techniques are lacking in security aspect. Biometric system utilize in various system for the identification or authentication approval. Biometric authentication system utilizes various biometric traits for the matching between various biometric traits. These feature values that have been computed by using various approaches for biometric traits like face, finger and iris. These feature values have been stored in database for matching purpose using distance classifier. After fusion these values has been computed for all the images present in the database and then test images has been selected and undergoes matching process on the basis of distance classifier. Min distance computed represents the maximum matching of the feature of different biometric traits. Parameter selected for the performance evolution of proposed system are FAR (False Acceptance Rate), FRR (False Rejection Rate) and ACCURACY.

Keywords: Bio-metrics, Multi-Thresholding

1. Introduction

Biometrics is combination of two Greek words Bios (life) and metrikos (measure). It is recognized that some human body characteristics such as face, gait or voice can be used to distinguish individual from a group of people. In a biometrics system a person is recognized on the basis of physical and behavioural traits. In it pattern recognition is used. In the process of pattern recognition human traits are captured on and then matched with the database. Biometric identifiers are the unique, measurable qualities used to mark and depict individuals. Biometric identifiers are regularly sorted as physiological versus behavioural characteristics. Physiological attributes are identified with the state of the body. Samples incorporate, however are not constrained to unique finger impression, palm veins, face recognition, DNA, palm print, hand geometry, iris distinction, retina and smell/fragrance. Behavioural attributes are identified with the example of conduct of an individual, including however not constrained to writing mood, walk, and voice. The primary thoughts of biometrics seemed numerous years back. By and large, it is extremely hard to say that biometrics showed up it this spot at this point. The thoughts to utilize parts of human body and even the approaches to utilize this thoughts seemed everywhere throughout the world. In the first place confirmations of biometrics showed up in 29.000bc when the cave dwellers utilized their fingerprints to sign their drawings. The initially recorded proof of utilizing biometric confirmation was as a part of old Egypt [11].

One of the executives, amid the development of extraordinary pyramid of Khufu, attempted to systemize the methodology of giving sustenance to specialists. He recorded all data about the specialist (name, age, work unit, position, occupation, and so on). Anyway afterward that numerous specialists swindled him, the head started to record the physical and behavioural qualities. In fourteenth century in China biometric confirmation was somewhat prominent among vendors [6].

Innovation of ahead of schedule biometrics was fairly straightforward: paper with ink permitted to take palm print s and foot shaped impressions of youngsters so as to separate them from other. It is fascinating to bring up that despite its effortlessness thusly of bimetric validation is still being used and is the most popular.

2. Characteristics of Biometrics

Any physical and/or behaviour characteristics of a human can be considered as a biometric if it exhibits following characteristics:
- **Universality:** Each person accessing the biometric application should posses a valid biometric trait.
- **Uniqueness:** The given biometric trait should exhibits distinct features across individuals comprising the population.
- **Permanence:** The biometric characteristics should remain sufficient invariant over a period of time.
- **Measurability:** The biometric characteristics can be quantitatively measured i.e. acquiring and processing of biometric trait should not cause inconvenience to the individual.
- **Performance:** The biometric trait should the required accuracy imposed by the application[12]

3. Types of Biometric Systems

Biometric system is broadly categorized in two types: Physical and Behavioural [7] (Jain et al. 2010):

**Physical Biometrics**
- Finger print Recognition
- Facial Recognition
- Hand Geometry
IRIS Recognition
DNA

Behavioral Biometrics
Speaker Recognition
Signature
Keystroke
Walking style

4. Operations of a Biometric System

Based on the appliance, a biometric system may operate either in verification mode or identification mode [4] (Jain et al. 2004). In the verification mode, a person’s identity is validated through comparison between the captured biometric data and its own biometric templates stored in the database of the system. In such a system, an individual who is desirable of recognition gives a claim of identity, usually a PIN and a one-to-one comparison is done by the system to determine if claim is true or not [8] (Wayman 2001). In the identification mode, an individual is recognised by questing through the templates (stored in database) of all the users for a good match. Therefore, a one-to-many comparison is made by the system to establish the identity of a user (or negative response is given if the subject is not part of the system’s database) without a subject having to put the efforts for claiming his/her identity[8](Wayman2001).

5. Methodology

The whole process can be shown in the form of a flow diagram:

This paper presents a multimodal biometric system comprising the fusion of iris, fingerprint and face templates. The existence of iris and fingerprint images is firstly aggrandized using a series of pre-processing techniques which include segmentation and Iris Images Fingerprint Images Face Images Pre-processing i.e. Segmentation & Normalisation Pre-processing i.e. Segmentation & Normalisation Feature Extraction Feature Extraction Feature Extraction Information Fusion Calculation of Scores for
verifying the Genuine & the Imposter Validation/Classification. Below are ten data base images for the IRIS that we have selected for the system:

![Figure 4: Ten images of IRIS data](image)

6. Results & Discussion

After extraction of features from various biometric traits fusion of feature on the basis of score level has to be done. Fusion techniques are divided into two different categories which are score level fusion and rank level fusion. In proposed work score level fusion approach has been utilized. After fusion the feature has to be saved in a file for recognition and authentication purpose. Next we have matching database. Once the enrolment of data is done by generating unique id and user id, now we only need to select your database then it will automatically extract the features and verify it with the stored data. If data matches with any of the stored data then the name of the user appears. Graphic user interface developed for the purpose of matching process which has to be performed on the database. In this various controls has been used for different purposes. This image is use to represents extraction of face features from the test face database. After extraction of face features fusion of the all iris, finger and face feature has to be done on the basis of score level fusion approach. Distance classification done with the database on the basis of different distance classifier. This classifier computes the distance between the different features of database images and to the query image features. These features described the similarity between different biometric traits. Where the minimum distance has been computed that is most matched feature vector. From that particular feature vector name of the identity is fetched out.

![Figure 5: Fingerprint sample images](image)

![Figure 6: Input Iris Image for feature extraction](image)

![Figure 7: Input Finger Image for feature extraction](image)

![Figure 8: Histogram before equalization](image)

![Figure 9: After equalization](image)

![Figure 10: Graph FAR & FRR Percentage](image)
This graph is used to represent the reliability of a system. Reliability is defined as the amount of time in which our system works properly. The point where the FAR and FRR curves meet is the equal error rate. It is the common alternative to define the performance of the system.

Table displays experimental results for recognition with face image alone and with the fusion of all the three modalities i.e. face, fingerprint, and iris. The results are better when compared with the base paper as a new modality (iris) is added. A minimum FAR of 1.1% is attained as compared to 1.6% in case of face alone and maximum FAR is limited to 3.8% with the proposed methodology. The overall GAR% achieved for the fusion of face, fingerprint, and iris is 94% as compared to 89%.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>IRIS</th>
<th>Fingerprint</th>
<th>Face</th>
<th>Fusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAR</td>
<td>0.01</td>
<td>0.0037</td>
<td>0.1437</td>
<td>0.0148</td>
</tr>
<tr>
<td>FRR</td>
<td>0.0021</td>
<td>0.91</td>
<td>0.79</td>
<td>0.98</td>
</tr>
<tr>
<td>GAR</td>
<td>0.92</td>
<td>0.89</td>
<td>0.91</td>
<td>0.94</td>
</tr>
<tr>
<td>Area(PIXAL)</td>
<td>76800</td>
<td>72416</td>
<td>75002</td>
<td>74608</td>
</tr>
<tr>
<td>SD</td>
<td>0.9282</td>
<td>0.0579</td>
<td>0.0589</td>
<td>0.0085</td>
</tr>
<tr>
<td>Mean</td>
<td>1.14</td>
<td>1.77</td>
<td>1.17</td>
<td>1.77</td>
</tr>
<tr>
<td>Min</td>
<td>0.02</td>
<td>0.12</td>
<td>0.15</td>
<td>0.12</td>
</tr>
<tr>
<td>Max</td>
<td>2.55</td>
<td>2.54</td>
<td>2.14</td>
<td>2.54</td>
</tr>
<tr>
<td>ERROR RATE</td>
<td>0.991</td>
<td>0.384</td>
<td>0.422</td>
<td>0.099</td>
</tr>
</tbody>
</table>

7. Conclusion

Biometric system utilize in various system for the identification or authentication approval. Biometric authentication system utilizes various biometric traits for the matching between various biometric traits. Various approaches have been used for the extraction of features from various types of biometric traits. In the proposed work the biometric traits utilize are face, fingerprint and iris. Single Biometric trait system is fail to provide accuracy for the authentication of different identities because due to single biometric trait the chances of mismatching increases. So to overcome these disadvantages of single trait biometric system, multimodal biometric system come into existence. Multimodal biometric system use face, finger and iris images for the development of proposed system. Feature from each biometric credential has been extracted and fused on the basis of score level fusion to reduce feature dimension. Computation speed increases due to reduction in feature dimension of fused features. This proposed system provides accuracy of 100%. This provides better security than other biometric system because illegal availability of all the traits of single person is not available to match and perform any illegal operation. So one can conclude that multimodal biometric system provides better result as compare to single biometric trait system.

References


features” International Journal of Scientific & Technology Research , June 2012, VOLUME 1, ISSUE 5, ISSN 2277-8616 pp. 31-35


[18]The research and implementation of the method of pretreating the face images based on Open CV machine visual library” International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011, pp. 2719 – 2721, vol. 11.


