International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 No.2, Pages : 26-31 (2014)
Special Issue of ICACE 2014, Held on March 10, 2014 in Hotel Sandesh The Prince, Mysore, India

MULTIMODAL BIOMETRICS USING MOBILE PHONE

E.GOKULAKRISHNAN[1], S.ASHA[2]
1School Of Computing Science And Engineering ,VIT University –Chennai,India,Gokulakrishnan.e2013@vit.ac.in
[2]School Of Computing Science and Enggineering,VIT University-Chennai,India,Asha.s@vit.ac.in

Abstract : Today with greater advancement in mobile phone technologies capable of recognizing a biometric feature for recognizing an individual, our proposed model is based on multimodal biometrics using face and fingerprint. Multimodal gives a greater accuracy and security when compared to uni-modal biometrics. The match score is a measure of similarity between the input and template biometric feature vectors. In multimodal Biometrics system the fusion of the information can be done at various levels due to ease in combining and accessing the scores generated by different matchers. This paper focuses on the heterogeneous approach.

Key Words: Biometrics, Multimodal Biometrics, Face, Fingerprint, Fusion, Matching Score.

INTRODUCTION

Biometrics is constantly evolving technology which has been widely used in many official and commercial identification applications. The increased concerns in security during recent years have essentially resulted in more attention being given to biometric-based authentication techniques.

Biometrics is used to identify a unique physiological & behavioural characteristic of an individual user that can be automatically checked. Biometric traits can be classified into physiological and behavioral biometrics.
i)Physiological : Face, Fingerprint, Hand Geometry And Iris Recognition.
ii) **Behavioral:** Signature, Voice & keystroke, etc, .

Biometric Recognition task can be split in to two groups: Identification (1:N match) and Verification (1:1).

Need for Biometrics

Biometrics is more suited than the traditional recognition system for the following reasons:

- Convenient
- Password are not user-friendly
- Perceived as more secured
- Passive identification
- To ensure safety and security, thus reducing the crime rates

Types of Biometrics

Fig 1 gives the various biometrics used for identification and verification.

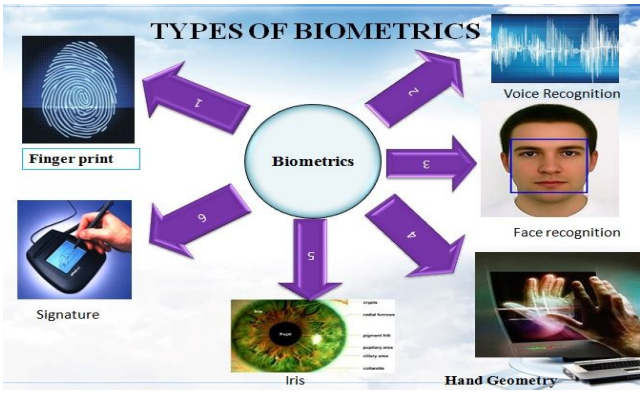

Fig 1: Types Of Biometrics

RELATED WORKS

Multimodal biometrics refers to the use of a combination of two or more biometric modalities in verification / identification system. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. One is that different biometric modalities might be more appropriate for the different applications.

The goal of multi-biometrics is to reduce one or more of the following:
• False accept rate (FAR)
• False reject rate (FRR)
• Failure to enroll rate (FTE)
• Susceptibility to artifacts or mimics

Multimodal

Biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example, a system combining face and iris characteristics for biometric recognition would be considered a “multimodal”[2]. Adaptive combination of multiple biometrics are used to ensure optimal performance for the desired level of security.

Which Biometric Modalities to Fuse?

Multiple biometrics should be combined together to get a common score using certain technology. Fusion is one such technique which will combine the score from different biometrics and produce a single score. But the types of biometrics that need to fused can be referred from the following figure 2, which gives the various combination of multiple biometrics.

Voice, Face
Voice, Lip Movement
Voice, Face, Lip Movement
Fingerprint, Face
Fingerprint, Face, Voice
Fingerprint, Face, Hand Geometry
Fingerprint, Voice, Hand Geometry
Fingerprint, Hand Geometry
Facial Thermo gram, Face
Iris, Face
Palm print, Hand Geometry
Ear, Voice

Fig 2: Types Of Biometric Modalities To Fuse

PROPOSED MODEL

In the proposed model, face and fingerprint are considered for multimodal biometric authentication.

FACE RECOGNITION

Face recognition is a biometric which uses computer software to determine the identity of the individual. Face recognition falls into the category of non invasive biometrics

Face Recognition System structure

Image is an input of face recognition and the output is an identification or verification .We are going to focus on Ada boost face detection algorithm and cascade classifier combination to achieve an efficient method for Face recognition .

Ada boost face Detection

To achieve an highly proficient face detection, we use a method proposed by Viola and Jones [3]. Face Recognition focuses on three major components, first one is Integral Image, which represents the image of people to calculate the features more accurately. The second one is Adaboost algorithm introduced by Freund and Schapire in 1997, which can extract the most important features. The last component is 'cascade classifiers', that can eliminate the non-face regions in the first few stages.

Integral image

Given an image I, we define an integral image I`(x,y) by $I`(x`,y`) = \sum_{X<x`,Y<y`} I(x,y)$

The value of the integral image at a location (x,y) is the summation over all the left and upper pixel values of the original image I. fig 3 shows the integral image.

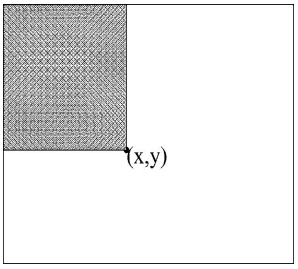

Fig 3: Integral Image [3].

If we have the integral image then we can define some rectangular features as shown in fig 4.

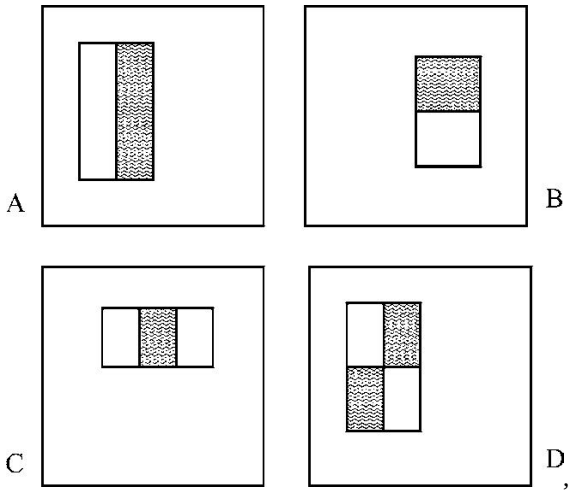

Fig 4: Rectangle feature [3]

The most commonly used features are 2, 3 & 4 rectangle features. The value of two-rectangle feature is the difference of the pixels sum over gray rectangle to the pixels sum over the white rectangle. These two regions have the same size and are horizontally or vertically adjacent as shown in blocks A and B. Block C is a three rectangle feature whose value is also defined as the difference of pixels sum over the gray region to the pixels sum over the white regions. Block D is an example of the 4-rectangle features. Since these features have used in different areas and it must be normalized after calculating the difference. After calculating the integral image in advance, it would be easy to obtain one rectangle region's pixels sum by one-plus operation and two-minus operations. For example, to calculate the sum of pixels within rectangle D in Figure 5, we can simply compute 4 + 1 – (2 + 3) value in the integral image.

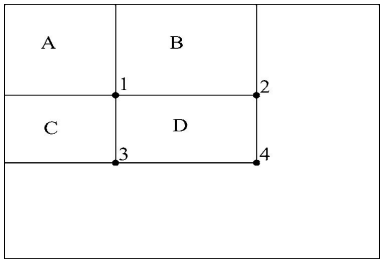

Fig 5: Rectangle sum[3]

AdaBoost

AdaBoost is an algorithm for constructing a strong classifier as linear combination .Here we are going to use an number of rectangle features with different size ,for example 24*24 pixel image there are 160000 features .

Adaboost is an machine learning algorithm used to find the T best classifiers with minimum error. To obtain the T classifiers. We will repeat the following algorithm given in Figure 6 for T number of iterations.

- Given example images $(x_1, y_1), \ldots, (x_n, y_n)$ where $y_i = 0, 1$ for negative and positive examples respectively.
- Initialize weights $w_{1,i} = \frac{1}{2m}, \frac{1}{2l}$ for $y_i = 0, 1$ respectively, where m and l are the number of negatives and positives respectively.
- For $t = 1, \ldots, T$:
  1. Normalize the weights, $w_{t,i} \leftarrow \frac{w_{t,i}}{\sum_{j=1}^{n} w_{t,j}}$
  2. Select the best weak classifier with respect to the weighted error
     $$\epsilon_t = \min_{f,p,\theta} \sum_i w_i \, |h(x_i, f, p, \theta) - y_i| \, .$$
     See Section 3.1 for a discussion of an efficient implementation.
  3. Define $h_t(x) = h(x, f_t, p_t, \theta_t)$ where f_t, p_t, and θ_t are the minimizers of ϵ_t.
  4. Update the weights:
     $$w_{t+1,i} = w_{t,i} \beta_t^{1-e_i}$$
     where $e_i = 0$ if example x_i is classified correctly, $e_i = 1$ otherwise, and $\beta_t = \frac{\epsilon_t}{1-\epsilon_t}$.
- The final strong classifier is:

$$C(x) = \begin{cases} 1 & \sum_{t=1}^{T} \alpha_t h_t(x) \geq \frac{1}{2} \sum_{t=1}^{T} \alpha_t \\ 0 & \text{otherwise} \end{cases}$$

where $\alpha_t = \log \frac{1}{\beta_t}$

Fig :6 Boosting Algorithm [3].
After Executing the Boosting algorithm for a ultimate goal object, we have T week classifiers with different weighting.at the end we get an strong classifier C(x).

Cascade Classifiers

Use of Cascade Classifier class is used to detect objects. Since we have the T best object detection Classifiers ,we can tune our cascade classifiers with user input the detection rate and the false positive rate. Figure 7 shows the algorithm for building cascade detector.

- User selects values for f, the maximum acceptable false positive rate per layer and d, the minimum acceptable detection rate per layer.
- User selects target overall false positive rate, F_{target}.
- P = set of positive examples
- N = set of negative examples
- $F_0 = 1.0$; $D_0 = 1.0$
- $i = 0$
- while $F_i > F_{target}$
  - $i \leftarrow i + 1$
  - $n_i = 0$; $F_i = F_{i-1}$
  - while $F_i > f \times F_{i-1}$
    - $n_i \leftarrow n_i + 1$
    - Use P and N to train a classifier with n_i features using AdaBoost
    - Evaluate current cascaded classifier on validation set to determine F_i and D_i.
    - Decrease threshold for the ith classifier until the current cascaded classifier has a detection rate of at least $d \times D_{i-1}$ (this also affects F_i)
  - $N \leftarrow \emptyset$
  - If $F_i > F_{target}$ then evaluate the current cascaded detector on the set of non-face images and put any false detections into the set N

Fig:7 Algorithm for building cascade detector [3]

Facial Features Detection and Extraction

Here is the innovative proposed method of the paper focus on how to extract the features of face recognition. Here we are going to use a gray level image with resolution 384*286 pixel. There are 9 manually marked features points as shown in figure 8.

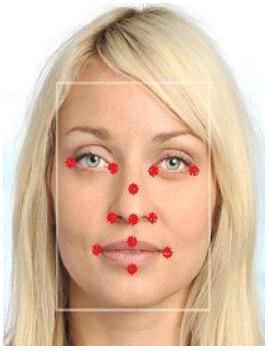

Fig 8:Face Features Detection

Here is the list of feature point:
0=right eye pupil
1=left eye pupil

2=midpoint of face
3=right nostril
4=left nostril
5=centre point of nostril
6=right mouth corner
7=left mouth corner
8=centre point on outer edge of upper lip
9=centre point on outer edge of lower lip
10=left temple
11=right temple

Here we are going to use adaboost algorithm to detect the face region in the image scale factor 1.05 to get a position as precise as possible, and then normalize the face size to calculate the feature relative position and their standard deviation. The original image and the detected face image and the features detected are shown in figures 10 and 11 respectively.

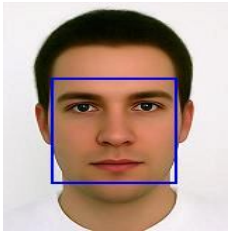

Fig 9: Original Image

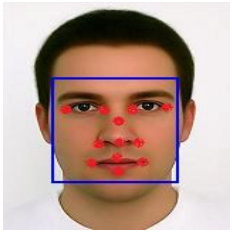

Fig 10: Face Detection and features marked

This is the proposed method for face detection and extraction. The following Table 1 is an example to find a feature position using standard deviation corresponding to x and y co-ordinates

Table 1: Four feature point extraction from face - Example.

	(pixel)	(pixel)	(pixel)	(pixel)
Landmark Index	X	Y	X st Dev	Y st Dev
0:right eye pupil	30.70	37.98	1.64	1.95
1:left eye pupil	68.86	38.25	1.91	1.91
2:right mouth corner	34.70	78.29	2.49	4.10
3:left mouth corner	64.68	78.38	2.99	4.15

FingerPrint Recognition

Fingerprint recognition or finger print authentication refers to the machine-driven technique of validating a match between 2 human fingerprints. Fingerprints square measure one in every of several varieties of life science want to determine people and verify their identity[5]. Finger print is one which is universally accepted for identification by life science.

The three main basic patterns of fingerprint ridges are the arch, loop, and whorl as shown in Figure 11.

- **Arch:** The ridges enter from one facet of the finger, and rise within the center forming Associate in Nursing arc, so exit the opposite facet of the finger.
- **Loop:** The ridges enter from one aspect of a finger, kind a curve, so exit thereon same aspect.
- **Whorl:** Ridges kind circularly around a central purpose on the finger.

About sixty five percentage of the full population has loops, thirty percentage have whorls, and five percentage have arches [6].

Fig 11: Types of patterns in finger print

Fingerprint Algorithm

In a fingerprint, the dark lines of the image are called the ridges and the white area between the ridges is called valleys[4]. This work is done applying several steps to achieve our goal:

- Collect many fingerprint image from different persons.
- Construct a particular fingerprint info.
- Classify the fingerprint in step with their characteristics.
- Construct the algorithmic rule to acknowledge the pattern.

Test the implemented algorithmic program to ascertain its accuracy [4]. The construction of the enforced algorithmic program is shown via many parts as shown in figure [12].

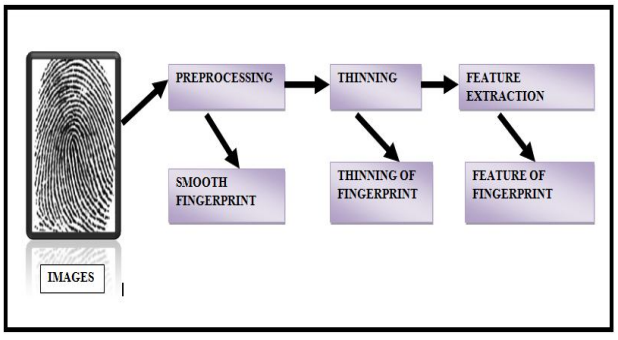

Fig 12: Component Of Fingerprint System

Preprocessing

It refers the process of preparing the input fingerprint ready for an execution stage which produces a good quality image. Preprocessing consists of the following steps.

- Image acquisition
- Convert input image in to grayscale,
- Remove unwanted image parts, image orientation in to exact position,
- Noise removal operation in which no effect on the fingerprint pattern.
- Image resizing into exact size. Image enhancement.

Thinning Process

The process of reducing the thickness of the lines to remove the spurious minutiae with minimum loss. It is used to identify the exact pattern of the fingerprint image.

Feature Extraction Process

It is the most sensitive method and target to illuminate the specified characteristics of the Minutiae. This may be enforced via trivialities detection and trivialities sweetening and detail extraction. Minutiae, in process terms, square measure the points of interest in an exceedingly fingerprint, like bifurcations and ridge endings [4]. Figure 13 shows the various processing stages of a fingerprint.

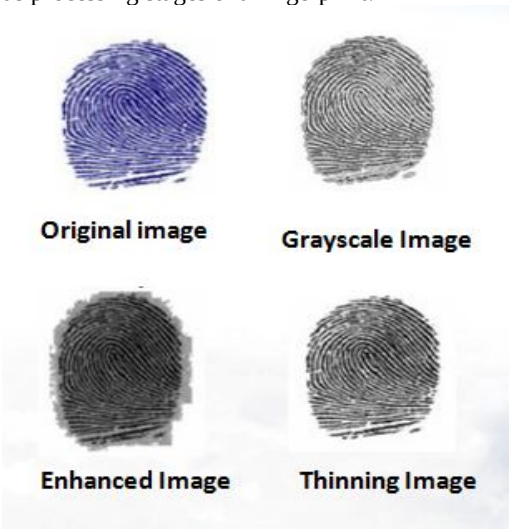

Fig13: Processing of Finger Print

This finger print extraction process provides more accuracy for comparison of fingerprints for matching.

Fusion in Multimodal Biometrics

In multi modal Biometrics we use more than one biometric modality;we have more than one decision channels.we need to design a mechanism that can combine the classification of result from each biometric channel ;this is called biometric fusion. Multimodal Biometrics have 4 modules:

Sensor level Fusion

In this module data is captured from the sensors .The obtained traits are combined to form a composite biometric trait.

Feature Level Fusion

In feature level fusion Signals coming from different traits are preprocessed and then fusion specific algorithm is used to obtain composite vectors,which is again used for classification .

Matching score module

Instead of combining feature vector each matching is done individually then fusion is done to obtain composite matching score .Composite matching score which will be used for classification.

Decision Level Fusion

Each Modality is first pre classified independently .The final Classification is based on the fusion of the outputs of the different modalities.

Multimodal biometrics system can implement any of these fusion strategies or combination of them to improve the performance of the system.

In this proposed model of the paper focuses on Score level fusion technique which uses the simple sum of raw score from individual biometrics.

Simple sum of of raw scores

Match scores are simply added ,with no prior normalization .scores are neither rescaled,nor weighted to account for differences in matcher accuracy .included largely to demonstrate its limited execution,which includes situations where scores have comparable distributions,such as two fingers scored by one matcher

Fusion At Matching Score Level

The following Figure 14 shows how the fusion of the biometrics Recognition using face and finger print is carried out. Initially both the face and finger print features have captured, each user have an match score individually by using fusion in matching score module generate an Fused score for an individual user according to that the person has identified whether he is Genuine or an Imposter .

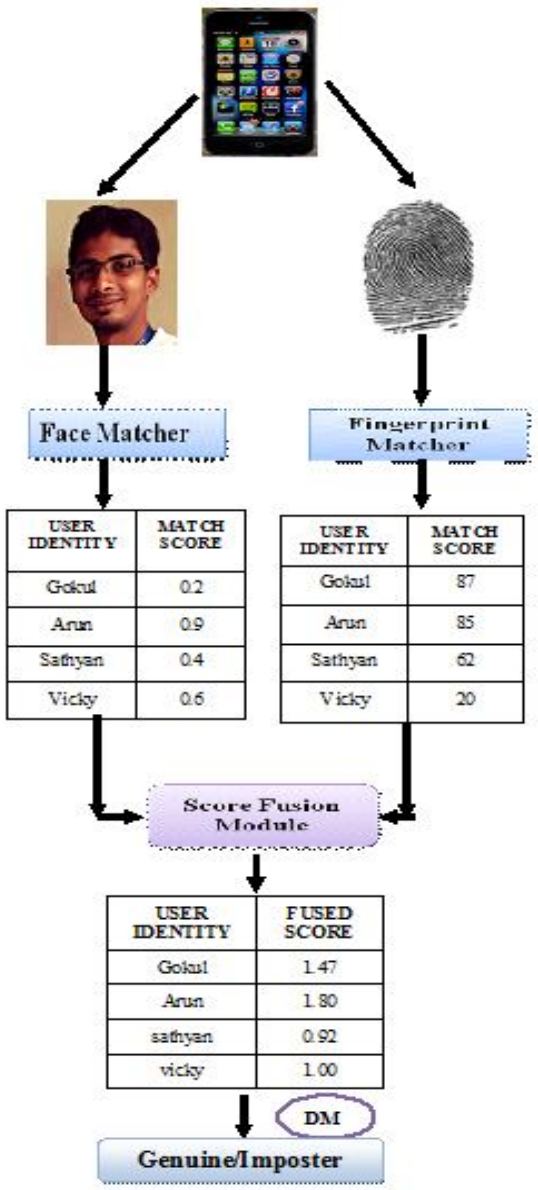

Fig:14 How the Fusion is Done in mobile Environment
DM:Decision Module

CONCLUSION

The performance of single modality primarily based biometric recognition has been tormented by the various creaky information, non-universality of biometric information, and susceptibleness of spoofing. The multimodal biometric system will improve the performance of the system. during this paper shows that face and finger print primarily based bimodal biometric system will improve the accuracy rate i Stongly advocate if we tend to use Multimodal biometrics(Face &Finger Print) The accuracy rate can even be im-proved victimisation advanced pattern recognition techniques, which can be used in future.

REFERENCES

[1] Jain A.K,Ross A. and Prabhakar S.(2009)IEEE Transactions on Circuits and systems for video technology ,14,4-20.
[2]. Ashish Mishra "Multimodal Biometrics it is: Need for Future Systems"Volume 3 – No.4, June 2010, International Journal of Computer Applications (0975 – 8887)
[3]P.Viola and M.J.Jones,"Robust Real-Time face Detection,",International journal of Computer Vision Vol.57,No. 2,pp.137-154,2004.
[4]. A Novel Thinning Algorithm for Fingerprint Recognition Muzhir Shaban Al-Ani,Anbar University – Anbar – Iraq.
[5]. http://en.wikipedia.org/wiki/Fingerprint_recognition .
[6].Sharath Pankanti, "On the Individuality of Fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, No.8, August
2002.