ANNEXURE - I

This research work is the experimentation of Multimodal Biometric Authentication System (MMBAS) which combines multiple biometric traits. In this regard the datasets that have been used in this research work is taken from various databases based on requirement. Three biometric traits have been used in this research work; face, finger and finger knuckle print and the database used for these traits are discussed as follows.

A.I.1 DATABASE FOR FACE RECOGNITION SYSTEM

Face recognition is one of the most challenging areas in the field of computer vision. Face detection is the first step for face recognition in order to localize and to extract the face region from the background. The system used local and Indian face database (IITK) for the experiment.

Local Face Database

This face database comprises 50 images from 25 persons. There are 15 females and 10 males, each of whom has two images (xa and xb) with different facial expressions. The xa images are used as gallery for training while the xb images as probes for testing. All the images are randomly selected from the local face database. Figure A.I.1 shows the sample images in local database.

![Sample Images from Local Face Database](image)

Figure A.I.1 Illustration of sample images from local face database

The development of face recognition over the past years allows into three types of recognition algorithms, namely frontal, profile, and view-tolerant recognition, depending on both kind of imagery (facial views) available, and according to the recognition algorithms.
Modern face recognition has reached an identification rate of greater than 90% for larger databases with well-controlled pose and illumination conditions.

Indian Face Data Base (IITK)

The database contains a set of face images taken in February, 2002 in the IIT Kanpur campus. There are eleven different images of each of 40 distinct subjects. For some subjects, some additional photographs are included. All the images were taken against a bright homogeneous background with the subjects in an upright, frontal position. The files are in JPEG format. The size of each image is 640x480 pixels, with 256 grey levels per pixel. The images are organized in two main directories - males and females. In each of these directories, there are directories with name as a serial numbers, each corresponding to a single individual. In each of these directories, there are eleven different images of that subject, which have names of the form abc.jpg, where abc is the image number for that subject. The following orientations of the face are included: looking front, looking left, looking right, looking up, looking up towards left, looking up towards right, looking down. Available emotions are: neutral, smile, laughter, sad/disgust. Sample images in IITK database:

Figure A.I.2 Illustration of sample images from Indian face database - IITK
There are many face databases are used in biometric authentication system like FERET, YALE, AR, IITK face database etc. Compared to other, IITK face database contains only Indian images which perform better results in Indian voting system through online. FERET database consists of face images of persons from different nationality in varying poses and times. It contains 261 images in $+15^\circ$ pose, among which 100 are used for learning the transformation matrix and 161 are used for testing. Contains 423 images in $\pm15^\circ$ pose, among which 50 are used for learning the transformation and 373 are used for testing. Unlike IITK database which contains only Indian face images, it contains face images of people from different nationality including blacks, whites, asians, caucasians, etc. Hence, results not as good as IITK Database. So, this research work uses Indian face database (IITK) for the experiment.

For face recognition, facial feature extraction algorithm is widely used. The distinguishing features found by the algorithm are used to compare images. There exist several algorithms to extract features such as Principal Component Analysis (PCA), Fisher Linear Discriminate Analysis (FLDA), Image principal component analysis (IPCA), Elastic Bunch Graph Matching (EBGM) and various others. This type of feature extraction algorithms needs manual interaction and do not consider prominent local features of a face, i.e., extracts the various facial features globally. Hence, it has the disadvantage over time and accuracy. So, the fast and computer visions algorithms like HOG, SIFT, MSER, k-means, hierarchical k-means, agglomerative information bottleneck, SLIC superpixels, and quick shift is carried out in the current research.

Automatic recognition is a vast and modern research area of computer vision, reaching from recognition of faces, facial expressions and gestures over related topics such as automatically detecting, locating and tracking faces, as well as extraction of face orientation and facial features, to such supporting fields as the handling of uncontrolled and uncontrollable conditions like illumination and shadows, and the 3D reconstruction of faces in particular, or the generation of new views from given imagery in general.
Finger Print Verification Competition 2004 (FVC2004)

Continuous advances in the field of biometric systems and, in particular, in fingerprint-based systems (both in matching techniques and sensing devices) require that the performance evaluation of biometric systems be carried out at regular intervals.

The aim of FVC2004 is to track recent advances in fingerprint verification, for both academia and industry, and to benchmark the state-of-the-art in fingerprint technology.

This competition should not be viewed as an “official” performance certification of biometric systems, since:

- The databases used in this contest have not been necessarily acquired in a real-world application environment and are not collected according to a formal protocol
- Only parts of the system software will be evaluated by using images from sensors not native to each system

Nonetheless, the results of this competition will give a useful overview of the state-of-the-art in this field and will provide guidance to the participants for improving their algorithms.

Participants

- Participants can be from academia or industry
- Anonymous participation will be accepted: participants will be allowed to decide whether or not to publish their names together with their system's performance. Participants will be confidentially informed about the performance of their algorithm before they are required to make this decision. In case a participant decides to remain anonymous, the label "Anonymous organization" will be used, and the real identity will not be revealed.
Organizers of FVC2004 will not participate in the contest. Four different databases (DB1, DB2, DB3 and DB4) were collected by using the following sensors/technologies:

- DB1: optical sensor "V300" by CrossMatch
- DB2: optical sensor "U.are.U 4000" by Digital Persona
- DB3: thermal sweeping sensor "FingerChip FCD4B14CB" by Atmel
- DB4: synthetic fingerprint generation

Note: FVC2004 databases are markedly more difficult than FVC2002 and FVC2000 ones, due to the perturbations deliberately introduced (see below). Therefore one should neither compare error rates among different FVC competitions, nor conclude that the state-of-the art in fingerprint matching is not improving. Students (24 years old on the average) enrolled in the Computer Science degree program at the University of Bologna kindly agreed to act as volunteers for providing fingerprints:

- Volunteers were randomly partitioned into three groups of 30 persons; each group was associated to a DB and therefore to a different fingerprint scanner (different subjects in each database, except for a small overlap of five volunteers present in two databases);

- Each volunteer was invited to present him/herself at the collection place in three distinct sessions, with at least two weeks time separating each session;

- Forefinger and middle finger of both the hands (four fingers total) of each volunteer were acquired by interleaving the acquisition of the different fingers to maximize differences in finger placement;

- No efforts were made to control image quality and the sensor platens were not systematically cleaned;

- At each session, four impressions were acquired of each of the four fingers of each volunteer;
During the first sessions, individuals were asked to put the finger at a slightly different vertical position (in impressions 1 and 2) and to alternate low and high pressure against the sensor surface (impressions 3 and 4);

During the second session, individuals were requested to exaggerate skin distortion (impressions 1 and 2) and rotation (3 and 4) of the finger;

During the third session, fingers were dried (impressions 1 and 2) and moistened (3 and 4).

At the end of the data collection, for each database a total of 120 fingers and 12 impressions per finger (1440 impressions) were gathered. As in previous editions, the size of each database to be used in the test was established as 110 fingers wide (w) and 8 impressions per finger deep (d) (880 fingerprints in all); collecting some additional data gave a margin in case of collection / labeling errors. Table A.I.1 shows the various database of finger print system.

<table>
<thead>
<tr>
<th>Data Base</th>
<th>Sensor Type</th>
<th>Image Size</th>
<th>Set A(wxd)</th>
<th>Set B(wxd)</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB1</td>
<td>Optical Sensor</td>
<td>640x480 (307Kpixels)</td>
<td>100x8</td>
<td>10x8</td>
<td>500 dpi</td>
</tr>
<tr>
<td>DB2</td>
<td>Optical Sensor</td>
<td>328x364 (119Kpixels)</td>
<td>100x8</td>
<td>10x8</td>
<td>500 dpi</td>
</tr>
<tr>
<td>DB3</td>
<td>Thermal sweeping Sensor</td>
<td>300x480 (144Kpixels)</td>
<td>100x8</td>
<td>10x8</td>
<td>512 dpi</td>
</tr>
<tr>
<td>DB4</td>
<td>SFInGe v3.0</td>
<td>288x384 (108Kpixels)</td>
<td>100x8</td>
<td>10x8</td>
<td>about 500 dpi</td>
</tr>
</tbody>
</table>

Fingers from 101 to 110 (set B) have been made available to the participants to allow parameter tuning before the submission of the algorithms; the benchmark is then constituted by fingers numbered from 1 to 100 (set A). Figure A.I.3 shows a sample image from each database:
A minimal training of the volunteers has been performed before the first acquisition session and failure to acquire has been measured during the three sessions, counting the number of attempts required to acquire a valid sample. Table A.I.2. shows the average number of acquisition attempts in training period.

**Table A.I.2. Average number of acquisition attempts in training period**

<table>
<thead>
<tr>
<th>Database</th>
<th>Sensor</th>
<th>Average number of acquisition attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB1</td>
<td>&quot;V300&quot; by CrossMatch</td>
<td>1.00</td>
</tr>
<tr>
<td>DB2</td>
<td>&quot;U.are.U 4000&quot; by Digital Persona</td>
<td>1.05</td>
</tr>
<tr>
<td>DB3</td>
<td>&quot;FingerChip FCD4B14CB&quot; by Atmel</td>
<td>1.61</td>
</tr>
</tbody>
</table>

There are two categories will be organized using the same databases, they are different open category and light category.

- Each participant is allowed to submit only one algorithm to each category
- The open category has no limits on memory requirements and template size.

For practical testing reasons, the maximum response time of the algorithms is limited as follows: the maximum time for each enrolment is 10 seconds; the maximum time for each matching is 5 seconds. The test will be executed under Windows XP Professional O.S. on PC AMD Athlon 1600+ (1.41 GHz). Table A.I.3. Categories organized using same database.
Table A.I.3. Categories organized using same database

<table>
<thead>
<tr>
<th></th>
<th>Open Category</th>
<th>Light Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrol time limit</td>
<td>10 seconds</td>
<td>0.5 seconds</td>
</tr>
<tr>
<td>Match time limit</td>
<td>5 seconds</td>
<td>0.3 seconds</td>
</tr>
<tr>
<td>Model size limit</td>
<td>No limit</td>
<td>2 Kbytes</td>
</tr>
<tr>
<td>Allocated memory limit</td>
<td>No limit</td>
<td>4 Mbytes</td>
</tr>
</tbody>
</table>

Biometric systems that rely on the evidence of a single source of information for authentication (e.g., single fingerprint or face) are often affected by a variety of practical problems, such as noisy data (due to a dirty sensor or a poorly illuminated environment), large intra-class variations (e.g. different facial poses), non-universality, spoof attacks, and unacceptable error rates. Multiple biometrics can help to solve several practical problems, thus improving the recognition performance, increasing population coverage (e.g. to those not having a legible fingerprint) and providing anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously.

The light category is intended for algorithms conceived for light architectures and therefore characterized by low computing needs, limited memory usage and small template size. The maximum time for enrolment is 0.5 seconds and the maximum time for matching is 0.3 seconds. The test will be executed under Windows XP Professional O.S. on PC AMD Athlon 1600+ (1.41 GHz). The maximum memory that can be allocated by the processes is 4 MBytes. The maximum template size is 2 KBytes. A utility will be made available to the participants to test if their executable comply with the memory requirement.

There has been a substantial amount of work done on the multimodal fusion approaches: the key is the combination of the various biometric characteristics at the feature extraction, match score, or decision level. Feature level fusion (also known as pre-classification fusion) combines feature vectors at the representation level to provide higher dimensional data points; match score level fusion and decision level fusion (post-classification fusion) combine the individual scores from multiple classifiers and the accept or reject decisions of each biometric system, respectively.
This research work takes a database of 50 persons. The face and fingerprint database are collected for individuals by taking the image of 256x256 and resolution is set to 72 dpi. For the sake of the experiment, cropped face has been taken which covers face only and for the fingerprint, cropped fingerprint has been taken which covers ridges and lines. Decomposition is done by DWT. For fingerprint acquisition, optical or semi-conduct sensors are widely used. They have high efficiency and acceptable accuracy except for some cases that the user’s finger is too dirty or dry. However, the testing database for the proposed work is from the available fingerprints provided by FVC2004 (Fingerprint Verification Competition 2004). So no acquisition stage is implemented.

In the past three decades, many biometric characteristics have been investigated, including fingerprint, face, iris, retina, voice, gait and signature, etc. Researchers noticed that the texture in the outer finger surface, especially in the area around the finger joint, has the potential to do personal authentication. In addition, skin pattern on the finger-knuckle is highly rich in texture due to skin folds and creases, and hence, can be considered as a biometric identifier. Further, advantages of using FKP include rich in texture features, easily accessible, contact-less image acquisition, invariant to emotions and other behavioural aspects such as tiredness, stable features and acceptability in the society.

**The Hong Kong Polytechnic University (PolyU) Finger-Knuckle-Print Database**

Among various kinds of biometric identifiers, hand based biometrics has been attracting considerable attention. Recently, it is found that the finger-knuckle-print (FKP), which refers to the inherent patterns of the outer surface around the phalangeal joint of one’s finger, is highly unique and can serve as a distinctive biometric identifier. Abundant line-like textures are contained in an FKP image.

The Biometric Research Centre (UGC/CRC) at The Hong Kong Polytechnic University has developed a real time FKP capture device, and has used it to construct a large-scale FKP database. To advance research and to provide researchers working in the area of FKP recognition with a platform to compare the
effectiveness of various FKP recognition algorithms, we intend to publish our FKP database, making it freely available for academic, noncommercial uses.

Description of the PolyU FKP Database

FKP images were collected from 165 volunteers, including 125 males and 40 females. Among them, 143 subjects were 20–30 years old and the others were 30–50 years old. We collected samples in two separate sessions. In each session, the subject was asked to provide 6 images for each of the left index finger, the left middle finger, the right index finger, and the right middle finger. Therefore, 48 images from 4 fingers were collected from each subject. In total, the database contains 7,920 images from 660 different fingers. The average time interval between the first and the second sessions was about 25 days. The maximum and minimum intervals were 96 days and 14 days, respectively. Figure A.I.4 show the dataset samples available for FKP in PolyU database.

A.I.4. Dataset samples available for FKP in PolyU database
The originally captured images as well as the Region of Interest (ROI) images were available for research. Each folder is named as “nnn_fingertype”. “nnn” represents the uniqueness of the person. In each folder, the first 6 images (01~06) were captured in the first session and the later 6 images (07~12) were captured in the second session (Lin Zhang et. al. 2011). The file names in each folder of originally captured images were named as nn_.jpg and the ROI images were named as nn_ROI.jpg where nn represents the serial number of the images (1–12) of one person. ROI images are contained in “FKP ROI.zip”.

The image size is 243 × 320 pixels, and an average of 230 SIFT features are extracted for each image. The raw faces were used without any kind of pre-processing (cropping, normalization, histogram equalization, etc.) to assess the robustness of the algorithms in the comparison. The data sets were standard images and taken for evaluating the proposed algorithm resulting using different evaluation metrics. The proposed technique is evaluated on greyscale images data sets of individuals where one slice was selected from images in the random to evaluate the performance of the proposed MMBAS.