AN APPROACH FOR IDENTIFICATION USING EAR AND FACE BIOMETRIC EMPLOYING SCORE BASED IMAGE FUSION DETECTION IN SURVEILLIANCE SYSTEM

Project Submitted in Partial Fulfillment of the Requirements
for the Degree of Bachelor of Technology in the Field of
Computer Science & Engineering

By

AKASH PAL

AVINANDAN SAU

DEBOLINA DAS

SUKANTA SHARMA

To

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

JIS COLLEGE OF ENGINEERING

(AFFILIATED TO WEST BENGAL UNIVERSITY OF TECHNOLOGY)

BLOCK ‘A’ PHASE ‘III’, NADIA – 741235

An approach for identification using ear and face biometrics employing score based image fusion and SIFT feature detection in Surveillance System

Project Submitted in Partial Fulfillment of the Requirements for the Degree of Bachelor of Technology in the field of Computer Science and Engineering

By
Akash Pal (12300111008)
Avianadan Sau (12300111030)
Debolina Das (12300111039)
Sukanta Sharma (12300111109)

Under the supervision
of
Mrs. Madhuchhanda Dasgupta

Department of Computer Science and Engineering
JIS College of Engineering
Block-A, Phase-III, Kalyani, Nadia, Pin-741235
West Bengal, India

May, 2015

JIS College of Engineering

Block 'A', Phase-III, Kalyani, Nadia, 741235
Phone: +91 33 2582 2137, Telefax: +91 33 2582 2138
Website: www.jiscollege.ac.in, Email: info@jiscollege.ac.in

CERTIFICATE

This is to certify that the thesis entitled “**An approach for identification using ear and face biometrics employing score based image fusion and SIFT feature detection in Surveillance System” submitted** by **Akash Pal, Avinandan Sau, Debolina Das & Sukanta Sharma** to the JIS College of Engineering for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** is a bona fide record of the work carried out by him under my / our supervision during the year 2014-2015. The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Mrs. Madhuchhanda Dasgupta
Asst. Professor
Dept. of Computer Science and Engineering
JIS College of engineering

Date: 21/05/2015

Prof. (Dr.) Sudarshan Nandy
HOD CSE Department

Principal
JIS College of Engineering

ACKNOWLEDGEMENT

The analysis of the project work wishes to express our gratitude to **Mrs. Madhuchhanda Dasgupta** for allowing the degree attitude and providing effective guidance in development of this project work. Her conscription of the topic and all the helpful hints, she provided, contributed greatly to successful development of this work, without being pedagogic and overbearing influence.

We also express our sincere gratitude to **Prof. (Dr). Sudarshan Nandy**, Head of the Department of Computer Science and Engineering of JIS College of Engineering and all the respected faculty members of Department of CSE for giving the scope of successfully carrying out the project work.

Finally, we take this opportunity to thank to **Prof. (Dr). S.K. Mitra**, Principal of JIS College of Engineering for giving us the scope of carrying out the project work.

Date: 21/05/2015

Akash Pal
B.Tech in Computer Science and Engineering
4thYear/8th Semester
Univ. Roll--12300111008

Avinandan Sau
B.Tech in Computer Science and Engineering
4thYear/8th Semester
Univ. Roll--12300111030

Debolina Das
B.Tech in Computer Science and Engineering
4thYear/8th Semester
Univ. Roll—12300111039

Sukanta Sharma
B.Tech in Computer Science and Engineering
4thYear/8th Semester
Univ. Roll--12300111109

LIST OF FIGURES

Figure	**Page No.**
Fig 1.1: Flow of Biometric Procedure	1
Fig 3.1: Side faces from CVL database	6
Fig 3.2: Face Profile Images	7
Fig 3.3: Ear Images	7
Fig 3.4: Operations within same octaves (same scale)	8
Fig 3.5: Operations between different octaves (different scale)	9
Fig 3.6: Orientation Assignment	10
Fig 3.7: The Key-point Descriptor	11
Fig 3.8: Face profile images with the SIFT features	11
Fig 3.9: Ear images with the SIFT features	12
Fig 3.10: Step 1 of matching	12
Fig 3.11: Step 2 of matching	13
Fig 3.12: Step 3 of matching	13
Fig 3.13: True match of first face-portion image	14
Fig 3.14: True Match of first ear images	14
Fig 3.15: False match of first face-profile image	15
Fig 3.16: False match of first ear image	15
Fig 3.17: Snapshot of the matching score of 10 users	17
Fig 3.18: Ideal FAR/FRR vs. Threshold curve	17
Fig 4.1: Levels of fusion	18
Fig 4.2: Sensor Level Fusion	18
Fig 4.3: Feature Level Fusion	19
Fig 4.4: Match Score Level Fusion	19
Fig 4.5: Rank Level Fusion	20
Fig 4.6: Decision Level Fusion	20
Fig 5.1: ROC curve of ear	21
Fig 5.2: FAR/FRR vs. Threshold curve for ear	21
Fig 5.3: DET curve for ear	22
Fig 5.4: ROC curve of face profile	22

Fig 5.5: FAR/FRR vs. Threshold curve for face profile	23
Fig 5.6: DET curve for face profile	23
Fig 5.7: ROC curve for sum	24
Fig 5.8: FAR/FRR vs. Threshold curve for sum	24

LIST OF TABLES

Tables	Page No
Table 6.1: Comparison between various techniques	25

INDEX

Acknowledgement i

List of Figures ii – iii

List of Tables iv

Abstract 1

1. Introduction 2 – 4
    1.1.Sensor Unit 2
    1.2.Feature Extraction Unit 2
    1.3.Matching Unit 3
    1.4.Matching and Decision Unit 3 – 4

2. Aim of the Project 5

3. Steps 6 -17
    3.1. Image Acquisition 6
    3.2.Region of Interest Extraction 7
    3.3.Feature Extraction 8 – 12
    3.4.Matching 12 – 15
    3.5.Performance Analysis 15 – 17

4. Fusion Techniques 18 – 20

5. Curves 21 – 24

6. Result 25

7. Conclusion 26

8. Code 27 – 33

9. References 34

10.Bibliography 35

ABSTRACT

Biometric surveillance is any technology which measures and analyses human physical and/or behavioural characteristic for authentication, or screening purposes. Identification is an essential part of our lives. Identification of authentic candidate is essential in E-Commerce, in keeping track of criminals, in airport and railway surveillance and many more aspects of the modern world. However identification of a person can be challenging especially when the person is not cooperating. This leads to classify the identification techniques broadly in to two categories: Passive and Active. In this current study an approach has been proposed combining the ear and face biometrics for the purpose of identification of a person using SIFT (Scale Invariant Feature Transform). The proposed multi biometric system achieves a recognition accuracy of 99.9958%.

Keywords: *SIFT, biometric fusion, ear-face biometric.*

1. INTRODUCTION

Biometrics are our most unique physical (and behavioural) features that can be practically sensed by devices and interpreted by computers so that they may be used as proxies of our physical selves in the digital realm. In this way we can bond digital data to our identity with permanency, consistency, and un-ambiguity and retrieve that data using computers in a rapid and automated fashion.

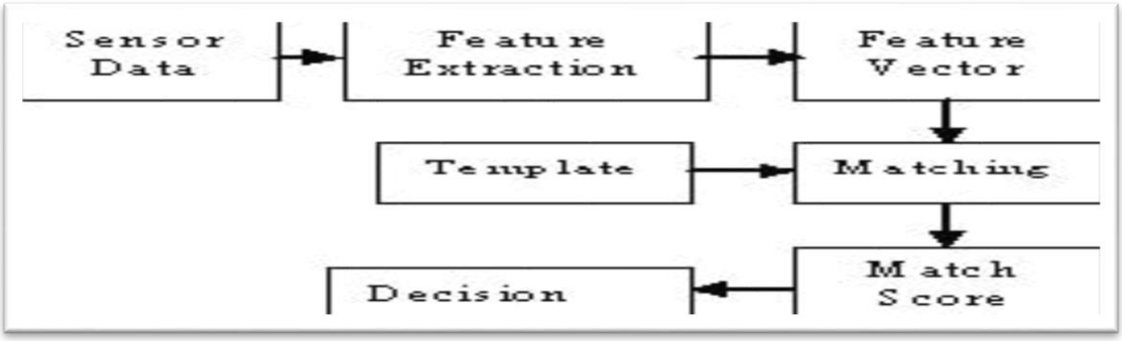


Fig 1.1: Flow of Biometric Procedure

1.1 Sensor Unit

This is where the biometric data is collected. The sensor unit is the most important stage because the accuracy of the entire system ultimately depends on the quality of data that is acquired by the unit.

For example in an Iris recognition system, the iris image may be affected by the illumination and by the distance between the camera and the eye.

1.2 Feature Extraction Unit

This is the stage where the data extracted by the sensor is analyzed, and the features that can be used to identify a person are extracted from the data. Each biometric trait has some features unique to the individual that can be used to identify a person. For example the fingerprint image has features such as whorls, arches, loops, ridges, furrows and minutiae. In iris recognition system, iris features such as rings, furrows and freckles in the colored tissues are used. There are a number of image processing algorithms that are available for feature extraction. The extracted features are represented as a vector, known as the feature vector. Next unit is the Matching unit, where the feature vector is matched with the other feature vectors that are stored in the database.

1.3 Matching Unit

The Matching unit can operate in two modes- verification mode or identification mode. In verification mode, we have to verify if the person is the one who he claims to be. So his biometric trait that was extracted is compared with the one stored in the database. This is basically a one to one matching process. In the identification process the extracted feature is compared to all the features that are stored in the database, which ever comparison gives the best result is taken as the match. So the identification process is a one to many matching process.

The core part of a good matcher is the database that is being used. Much research has been going on in data sharing among different organizations and organizing data in a common database. Biometrics products have to be standardized, so that the databases can be shared among different organizations. Some of the organizations that are working on the standardization of biometrics in the US and in the International front are International Biometric Group (IBG), International Committee for IT Standards, National Institute of Standards and Technology (NIST, standardizing fingerprint searches), International Civil Aviation Organization and Organization for the Advancement of Structured Information Standards (OASIS) [BIOREP].

In a biometric database, the data is stored in the form of templates, representing the biometric measurement of an enroller, and used by a biometric system for comparison against subsequently submitted biometric samples). So a template is formed using the extracted features from and individual and is compared with the once in the database.

1.4 Matching and Decision Unit

This is the unit that calculates the match between the templates. If the match is above a predefined threshold, then the template is said to be matching. This threshold depends on various factors like the person using the device, level of security that is needed, quality of the biometric trait that has been extracted, etc.

There are two types of biometric system:

A. Unimodal Biometric

In unimodal biometric system only one biometric trait is used for the purpose of identification of a person.

B. Multimodal Biometric

In multi-modal biometric system more than one biometric trait is used for the purpose of identification.

For instance iris recognition systems can be compromised by aging irises and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken pass-code).Multimodal biometric systems can integrate these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively.

Broadly, the information fusion is divided into three parts, pre-mapping fusion, midst-mapping fusion, and post-mapping fusion/late fusion. In pre-mapping fusion information can be combined at sensor level or feature level.

Sensor-level fusion can be mainly organized in three classes:

1. Single Sensor - Multiple Instances
2. Intra Class - Multiple Sensors
3. Inter Class - Multiple sensors

Feature-level fusion can be mainly organized in two categories:

1. Intra Class
2. Inter Class

Intra-class is again classified into four subcategories:

1. Same Sensor - Same Features
2. Same Sensor - Different Features
3. Different Sensors - Same Features
4. Different Sensors - Different Features

Spoof attacks consist in submitting fake biometric traits to biometric systems, and are a major threat that can curtail their security. Multi-modal biometric systems are commonly believed to be intrinsically more robust to spoof attacks, but recent studies have shown that they can be evaded by spoofing even a single biometric trait.

However unimodal biometric system has certain disadvantages due to which the multimodal biometric systems are preferred. There are two stages of a biometric system:

A. Enrolment

Enrolment is the process of the creation of users’ sample based on certain biometrics traits and storing it in the user database.

B. Authentication

During the authentication phase the identity of a user is verified by obtaining the biometric traits and comparing with the stored one. The user is accepted if it is an appropriate match.

2. AIM OF THE PROJECT

The aim of this project is very realistic. This project had been carried out some goals by which some real world scenarios can be solved.

There are mainly three objective of this project:

1. SIFT as the feature extraction algorithm.
2. Propose a new multi-biometric trait combining side-face and ear for a surveillance system.
3. Obtaining the accuracy of this proposed system.

In surveillance system, the objective is to identity an individual(s) successfully whose records are present in the database. The biometric traits have to be acquired passively. If only the face is captured then from this side face two biometric traits can be obtained the ear and a portion of the face. Since ear as a biometric system is not effective combining with the face-portion could give better result. In this paper, a database of side-faces is used to verify the effectiveness and the accuracy of the proposed system.

3. STEPS

There are five steps in this project:

1. Image Acquisition
2. Region of Interest Extraction
3. Feature Extraction
4. Matching
5. Performance Analysis

3.1 Image Acquisition:

For this purpose the CVL (Computer Vision Laboratory) face database has been used. It contains facial images of 114 subjects, with 7 images for each person. Each of the images was taken with a Sony Digital Mavica under uniform illumination, no flash and with projection screen in the background. All the images are of resolution 640 × 480 pixels in jpeg format.

All the subjects were mostly male (around 90%) around 18 (pupils and some professors). For this work, only one image (i.e. the side face) per subject is used. Out of 114 subjects only 109 subjects were considered as 5 of had occluded ear.

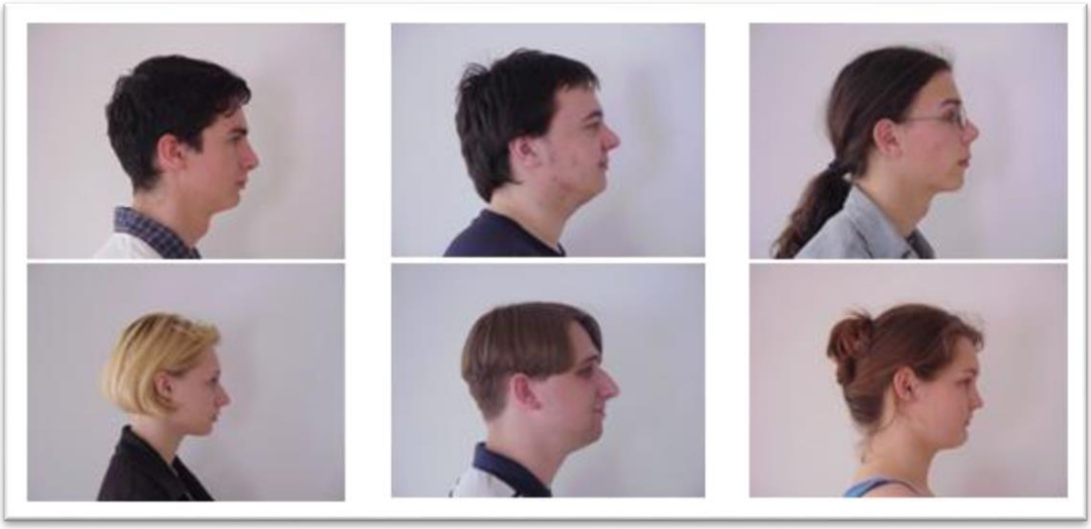


Fig 3.1: Side faces from CVL database

3.2 Region of Interest Extraction

The face and the ear of each person can be extracted automatically using techniques such as template matching. However, here the face and the ear of each person are extracted manually by cropping.

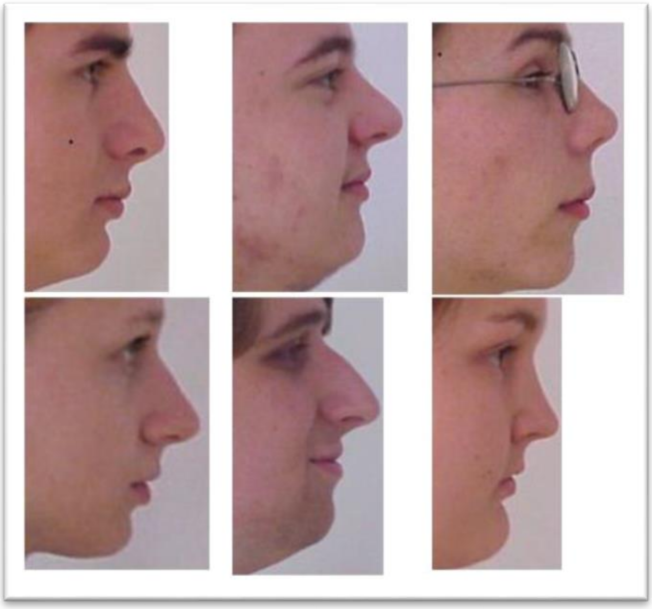


Fig 3.2: Face Profile Images

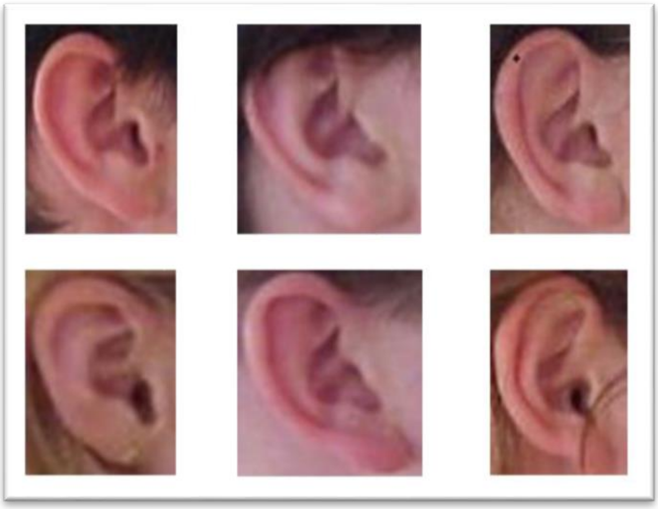


Fig 3.3: Ear Images

3.3 Feature Extraction

For the purpose of feature extraction the SIFT (Scale Invariant Feature Transform) algorithm proposed by D. Lowe [3] has been used.

3.3.1 SIFT Descriptor

The scale invariant feature transform, called SIFT [6] descriptor, has been proposed by and proved to be invariant to image rotation, scaling, translation, partly illumination changes. Following are the major stages of computation used to generate the set of image features.

3.3.2 Scale Space Extrema Detection

The first stage of computation is to create a scale of images. This is done by constructing a set of progressively Gaussian blurred images with increasing values of sigma. Then the difference between pairs of Gaussian is taken to obtain a Difference of Gaussian (DOG) which is similar to the function Laplacian of Gaussian (LOG) to obtain potential locations for finding features. The image is then sub-sampled (i.e. 1/4th resolution of lower octave) to obtain the next octave and the same process is repeated to obtain DOG pyramid.

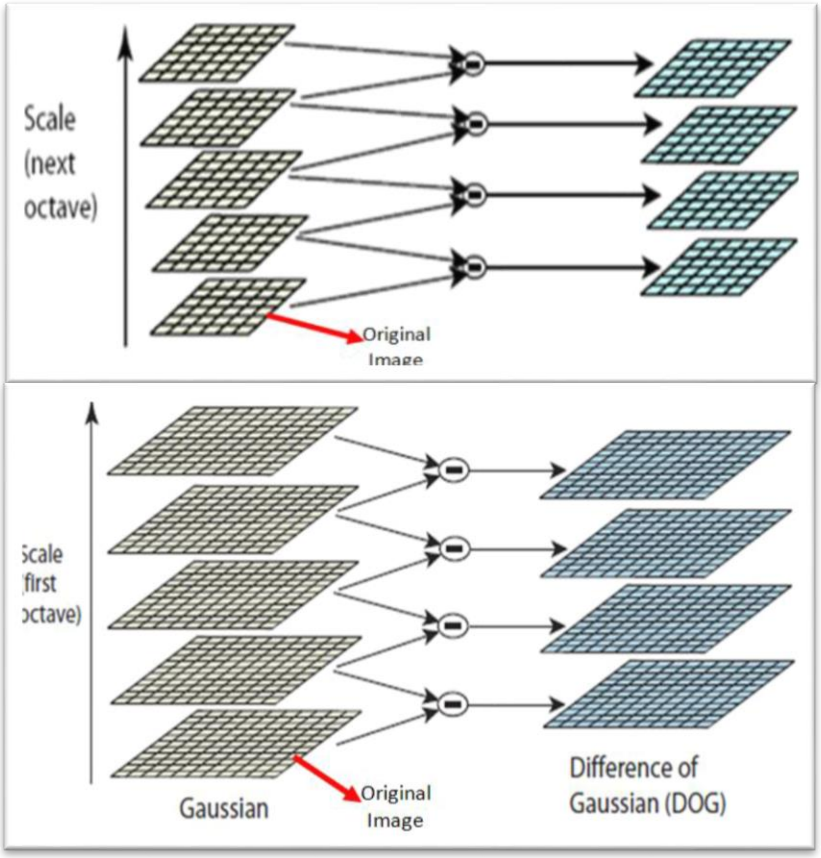


Fig 3.4: Operations within same octaves (same scale)

3.3.3 Key-point Localization

Accurately locates the feature key-points by comparing a pixel (X) with 26 pixels in current scale and adjacent scales (Green Circles). The pixel (X) is selected if it is larger/smaller than all 26 pixels. There are still a lot of points; some of them are not good enough. The locations of key-points may be not accurate. Eliminating edge points, key-point are selected from the extrema based on measures of their stability.

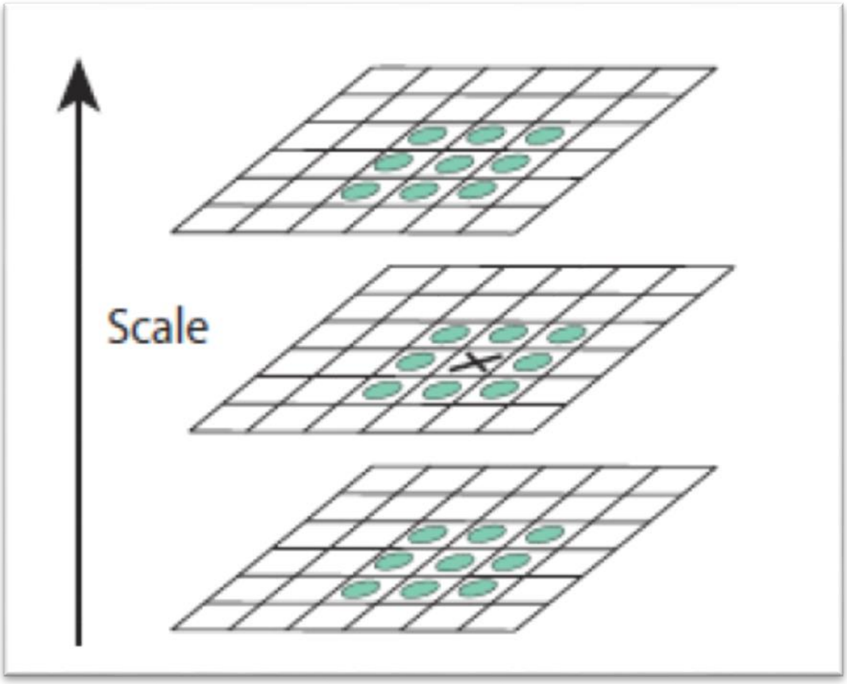
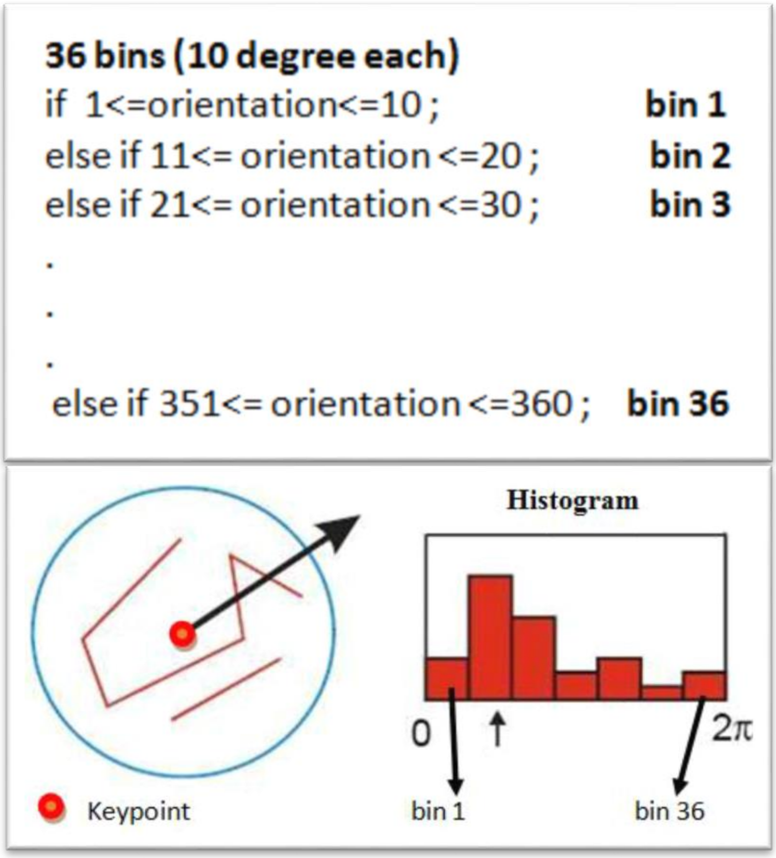


Fig 3.5: Operations between different octaves (different scale)

3.3.4 Orientation Assignment

This step assigns orientation to each key-point, the key-point descriptor can be represented relative to this orientation and therefore achieve invariance to image rotation. It computes magnitude and orientation on the Gaussian smoothed images. An orientation histogram is formed from the gradient orientations of sample points within a region around the key-point. Peaks in the orientation histogram correspond to dominant directions of local gradients. The highest peak in the histogram is detected, and then any other local peak that is within 80% of the highest peak is used to also create a key-point with that orientation. One or more orientations are assigned to each key-point location based on local image gradient directions.



```
36 bins (10 degree each)
if  1<=orientation<=10 ;                  bin 1
else if 11<= orientation <=20 ;           bin 2
else if 21<= orientation <=30 ;           bin 3
.
.
.
else if 351<= orientation <=360 ;         bin 36
```

Fig 3.6: Orientation Assignment

3.3.5 Key-point Descriptor

This step describes the key point as a high dimensional vector. The local image gradients are measured at the selected scale in the region around each key-point. It computes relative orientation and magnitude in a 16 x 16 neighbourhood around each key-point.

It forms weighted histogram (8 bin) for 4 × 4 regions. Finally it concatenates 16 histograms in one long vector of 128 dimensions.

These are transformed into a representation that allows for significant level of local shape distortion and change in illumination. This approach has been named the Scale Invariant Feature Transform (SIFT), as it transforms image data into scale invariant coordinates related to local features.

An important aspects of this approach is that is it generates large number of features that densely cover the image over the full range of scales and locations.

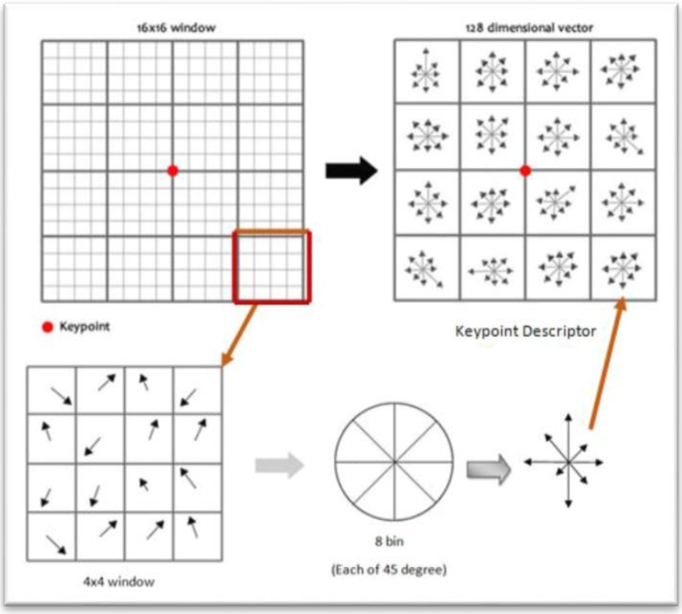


Fig 3.7: The Key-point Descriptor

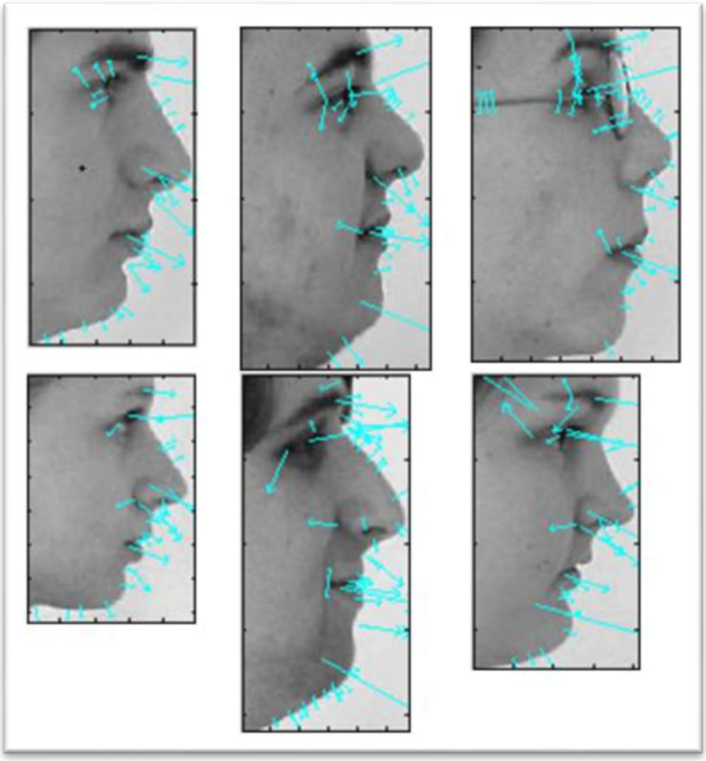


Fig 3.8: Face profile images with the SIFT features

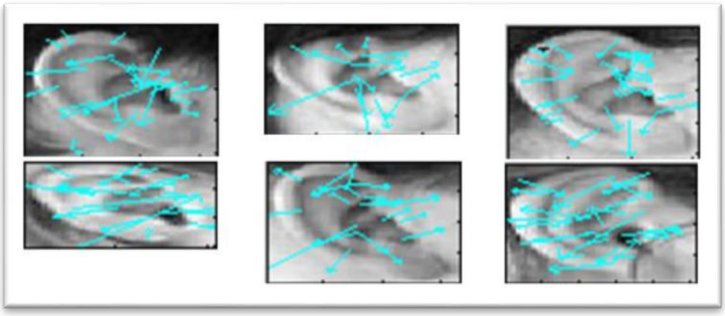


Fig 3.9: Ear images with the SIFT features

3.4 Matching

There are five steps of matching:

1. Before matching two images the feature description of the two images are obtained. Now for each descriptor in the first image, a match is selected in the second image.

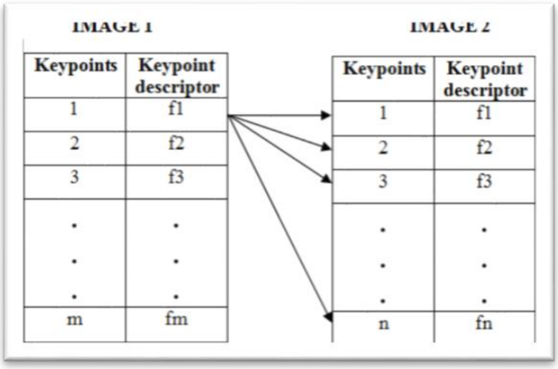


IMAGE 1

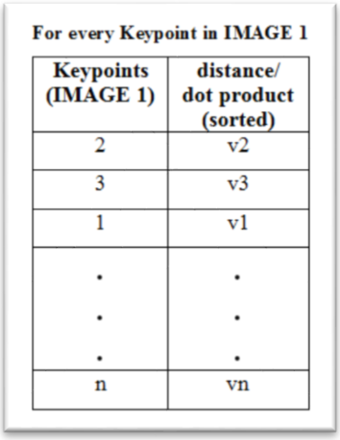
Keypoints	Keypoint descriptor
1	f1
2	f2
3	f3
. . .	. . .
m	fm

IMAGE 2

Keypoints	Keypoint descriptor
1	f1
2	f2
3	f3
. . .	. . .
n	fn

Fig 3.10: Step 1 of matching

2. For obtaining the match of the first key-point in the first image. The dot product is calculated between the first key-point descriptor in the first image with the other key-point descriptor in the second image and is denoted by v_1, v_2, v_3, ……, v_n. After calculating the dot product, the key-points are sorted in ascending order based on the dot product. This is done for every key-point in the first image.

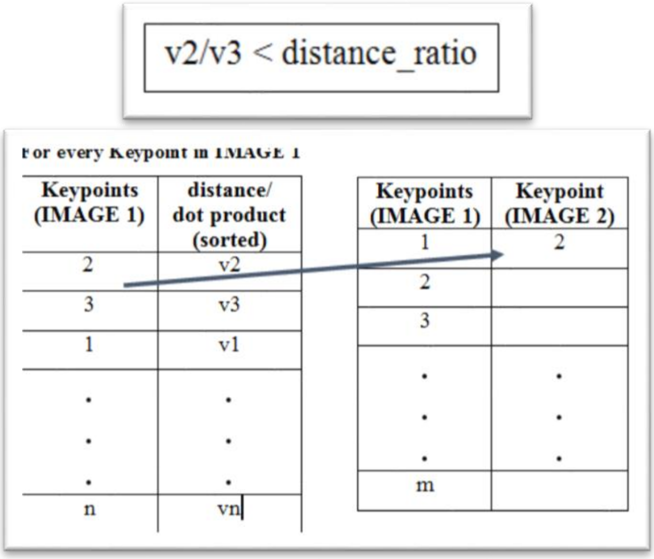


For every Keypoint in IMAGE 1

Keypoints (IMAGE 1)	distance/ dot product (sorted)
2	v2
3	v3
1	v1
⋮	⋮
n	vn

Fig 3.11: Step 2 of matching

3. In this step the ratio of the two smallest values in taken. If this value is less than the distance ratio then the first key-point in the sorted list is taken to be the matching key-point for the first key-point in first image.



v2/v3 < distance_ratio

For every Keypoint in IMAGE 1

Keypoints (IMAGE 1)	distance/ dot product (sorted)
2	v2
3	v3
1	v1
⋮	⋮
n	vn

Keypoints (IMAGE 1)	Keypoint (IMAGE 2)
1	2
2	
3	
⋮	⋮
m	

Fig 3.12: Step 3 of matching

4. This entire process is repeated for obtaining the matching key-points between the two images.
5. Finally the two images are appended side-by-side and then a straight line is drawn between the matched key-points. Also the matching score between the images is given.

There can be two types of matching:

A. True Match

When an image is matched against itself, it is called a **True Match**. In this case the number of key-points generated is large.

If the first face-portion image is compared with itself then 36 match points were found. Figure below shows the result of matching.

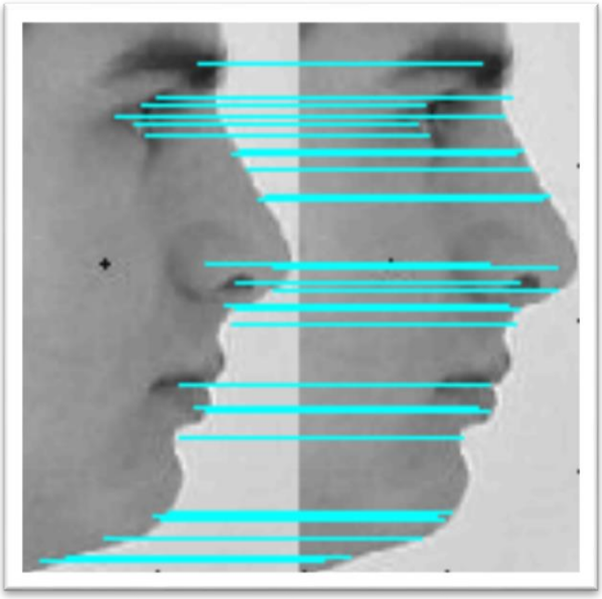


Fig 3.13: True match of first face-portion image

If the first ear image is compared with itself then 27 match points were found. Figure below shows the result of matching.

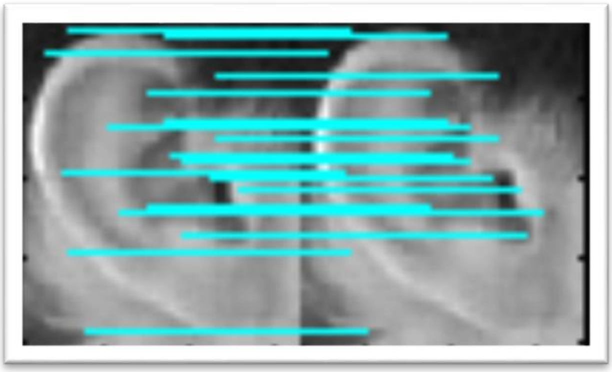


Fig 3.14: True Match of first ear images

B. False Match

When an image is matched against an imposter image, it is called a **False Match**. In this case the number of key-points generated is very less. If the face-portion image is compared with the second face-portion image then 3 match points were found. Figure below shows the result of matching.

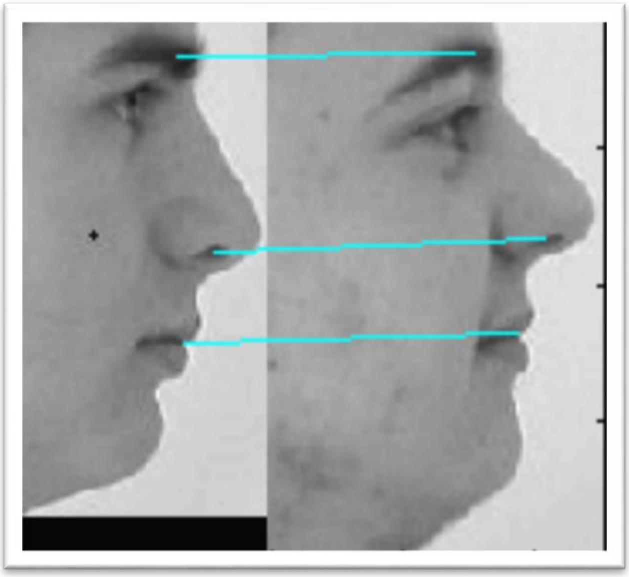


Fig 3.15: False match of first face-profile image

If the first ear image is compared with the second ear image then 0 match point was found. Figure below shows the result of matching.

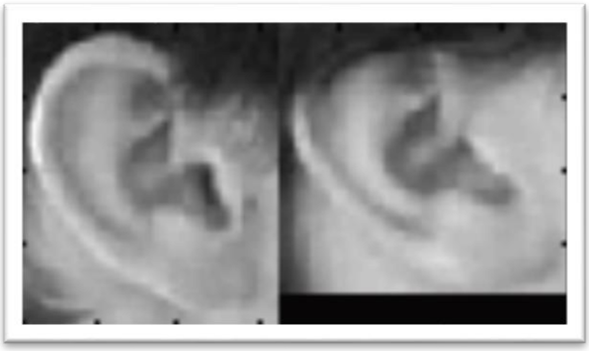


Fig 3.16: False match of first ear image

3.5 Performance Analysis

FRR (False Rejection Rate) is the process of falsely rejecting a genuine user.

$$FRR\ (False\ Rejection\ Rate) = \frac{Number\ of\ false\ Rejections}{Total\ number\ of\ authentic\ attempts}$$

FAR (False Acceptance Rate) is the process of falsely accepting an imposter.

$$\boxed{FAR\ (False\ Acceptance\ Rate) = \frac{Number\ of\ false\ Acceptance}{Total\ number\ of\ imposter\ attempts}}$$

EER (Equal Error Rate) is defined as the point where FAR is equal to FRR.

$$\boxed{ERR\ (Equal\ Error\ Rate) = \frac{FAR + FRR}{2}}$$

$$\boxed{EAccuracy = 100 - \mathrm{EER}}$$

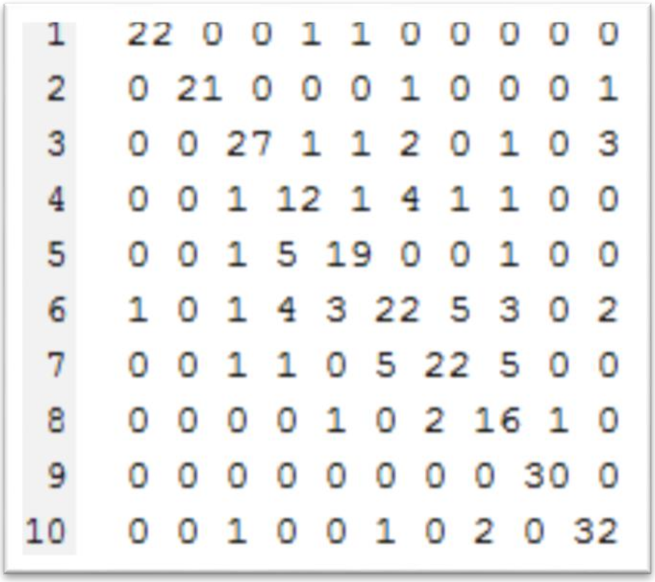
❖ Receiver Operating Characteristic (ROC) curve

This curve is used to summarize the performance of a biometric verification system. An ROC curve plots, parametrically as a function of the decision threshold, the percentage of impostor attempts accepted (i.e. False Acceptance Rate (Far)) on the x-axis, against the percentage of genuine attempts accepted (i.e. 1-False Rejection Rate (FRR)) on the y-axis. The ROC curve is threshold independent, allowing performance comparison of different systems under similar conditions.

❖ Detection Error Trade-off (DET) curve:

In the case of biometric systems, the DET curve is often preferred to the ROC curve. Indeed, the DET curve plots error rates on both axes (FAR on the x-axis against FRR on the y-axis) using normal deviate scale what spreads out the plot and distinguishes different well performing systems more clearly.

109 numbers of images are used from the CVL database. For finding **FRR** each image is compared against itself, which results in 190 authentic attempts into the proposed system. For finding **FAR** each image is compared with the other 108 image, which results in 11772 $(109 \times 109 - 109)$ imposter attempts into the proposed system. The FAR and FRR can be combined together into matching score matrix.

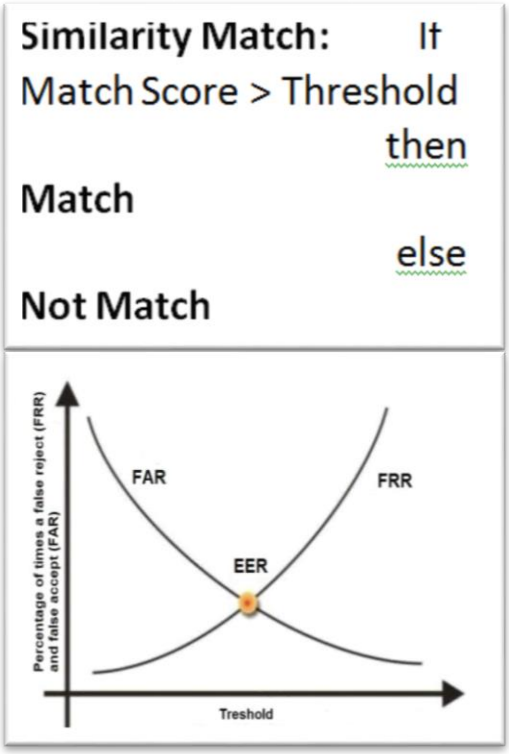


1	22	0	0	1	1	0	0	0	0	0
2	0	21	0	0	0	1	0	0	0	1
3	0	0	27	1	1	2	0	1	0	3
4	0	0	1	12	1	4	1	1	0	0
5	0	0	1	5	19	0	0	1	0	0
6	1	0	1	4	3	22	5	3	0	2
7	0	0	1	1	0	5	22	5	0	0
8	0	0	0	0	1	0	2	16	1	0
9	0	0	0	0	0	0	0	0	30	0
10	0	0	1	0	0	1	0	2	0	32

Fig 3.17: Snapshot of the matching score of 10 users

In this matrix the diagonal scores represents the FRR and the rest of the scores except the diagonal elements represents the FAR.

In case of similarity match, if the matching score is more that the matching score is more that the threshold then it is a match or else not.



Similarity Match: If
Match Score > Threshold
then
Match
else
Not Match

Fig 3.18: Ideal FAR/FRR vs. Threshold curve

4. FUSION TECHNIQUES

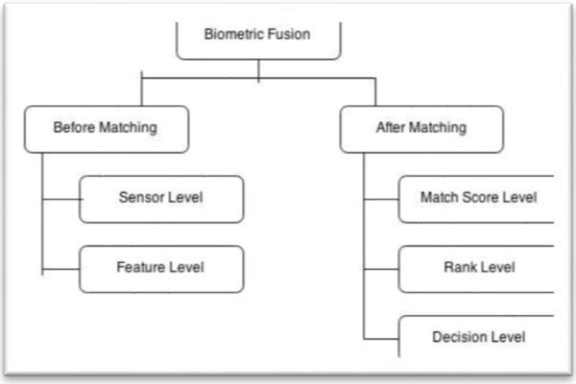


Fig 4.1: Levels of fusion

The diagrams of the fusion techniques are given below:

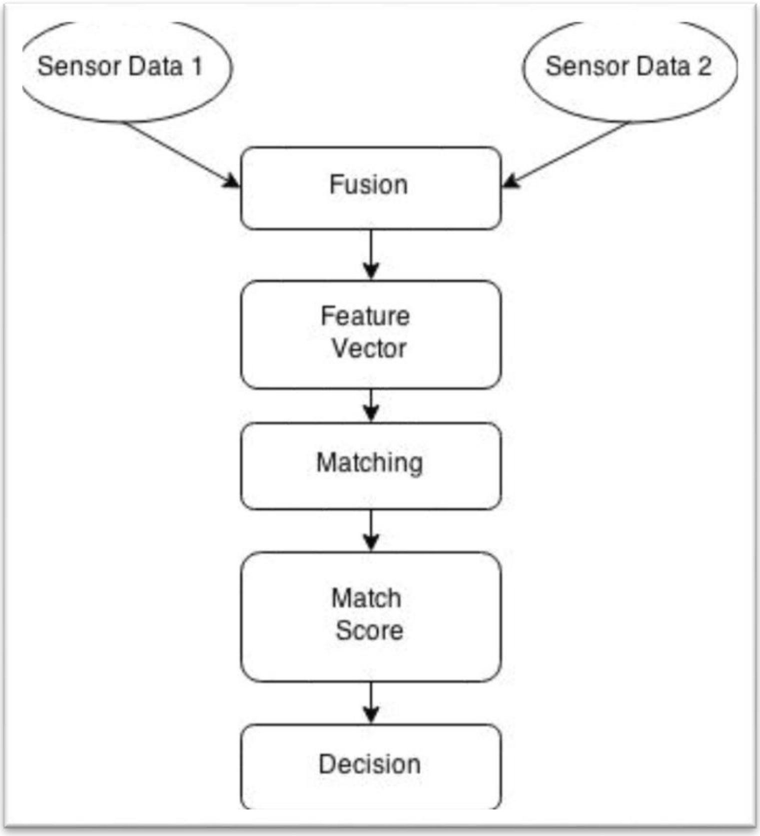


Fig 4.2: Sensor Level Fusion

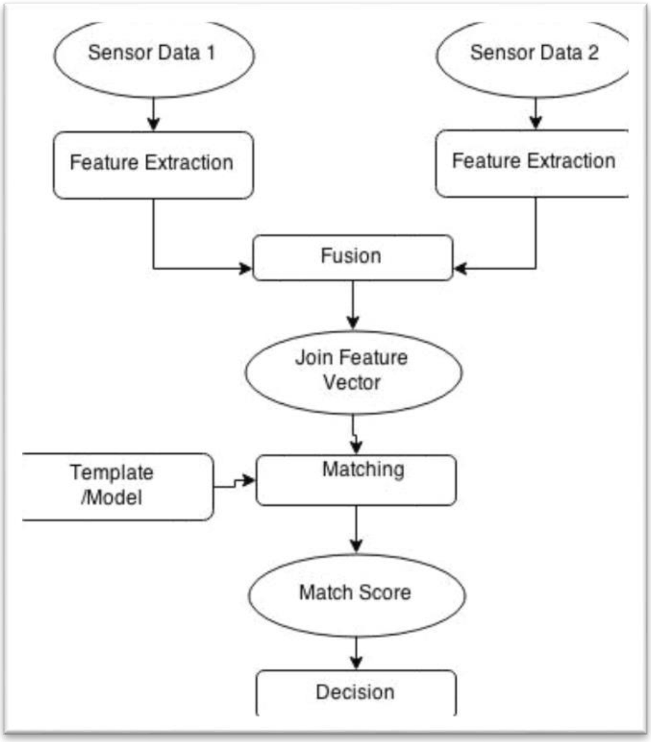


Fig 4.3: Feature Level Fusion

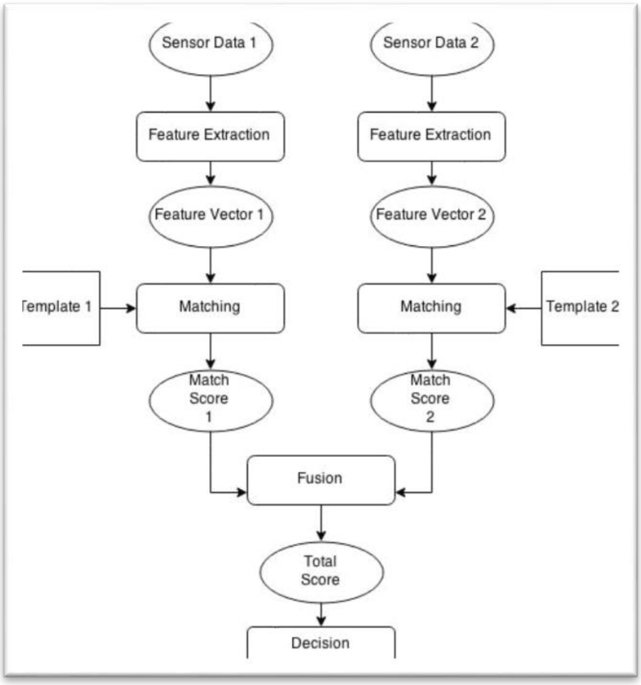


Fig 4.4: Match Score Level Fusion

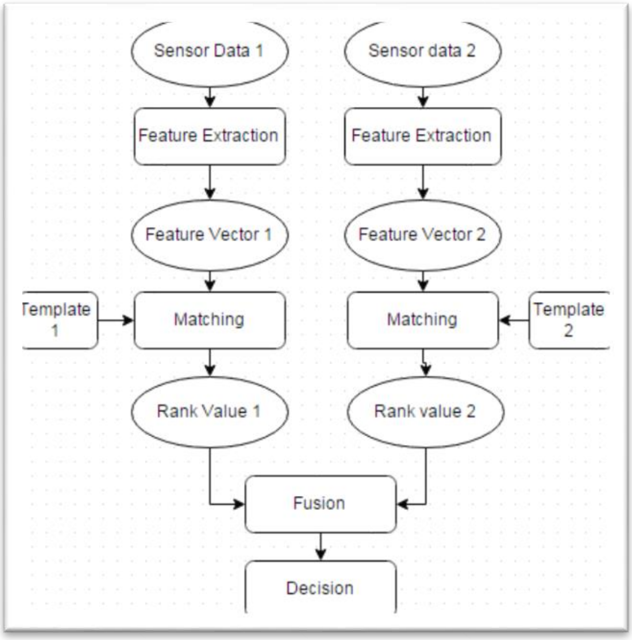


Fig 4.5: Rank Level Fusion

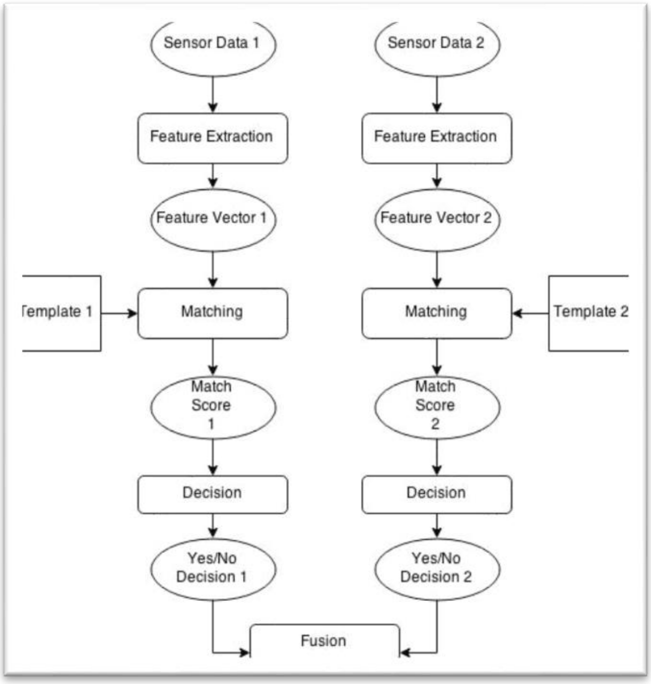


Fig 4.6: Decision Level Fusion

For the proposed system, the score level fusion technique has been adopted. The matching score matrix of ear and face-portion are combined together into a single matching score matrix using sum rule. This matching score matrix is used for performance analysis.

5. CURVES

5.1Ear Images

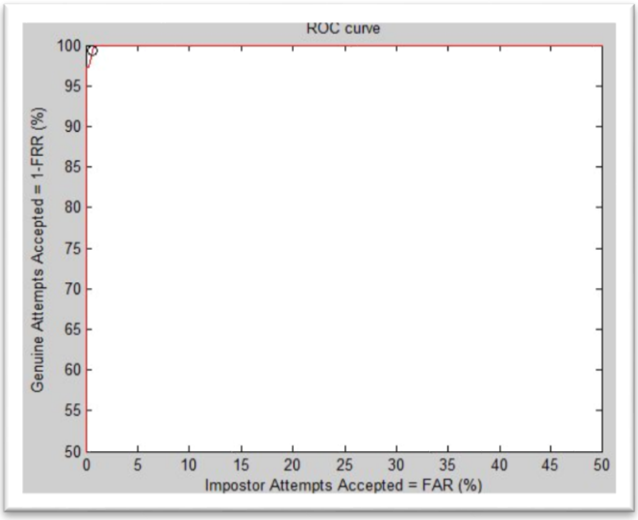


Fig 5.1: ROC curve of ear

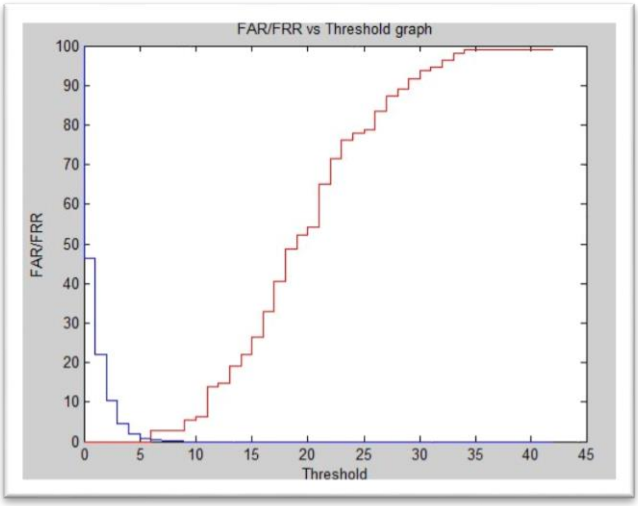


Fig 5.2: FAR/FRR vs. Threshold curve for ear

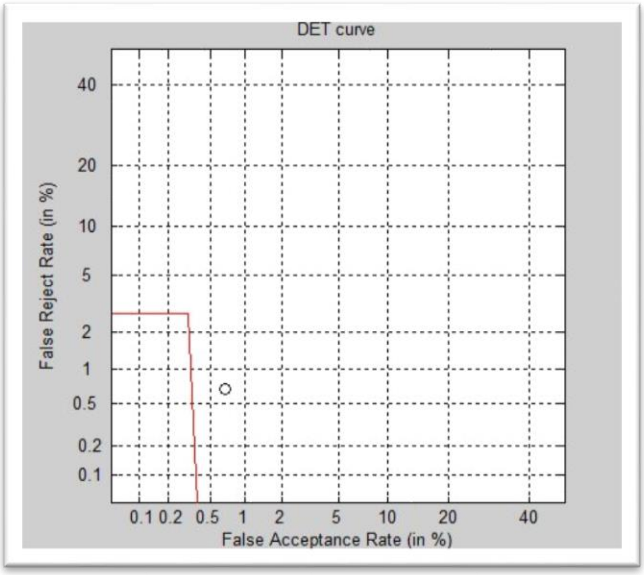


Fig 5.3: DET curve for ear

5.2Face Profile

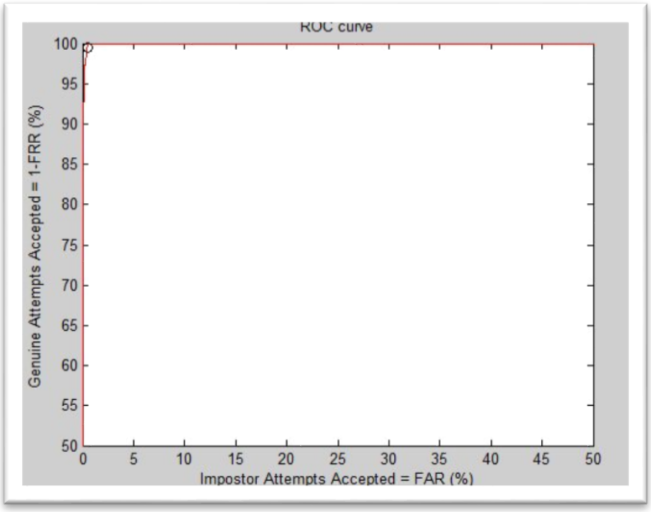


Fig 5.4: ROC curve of face profile

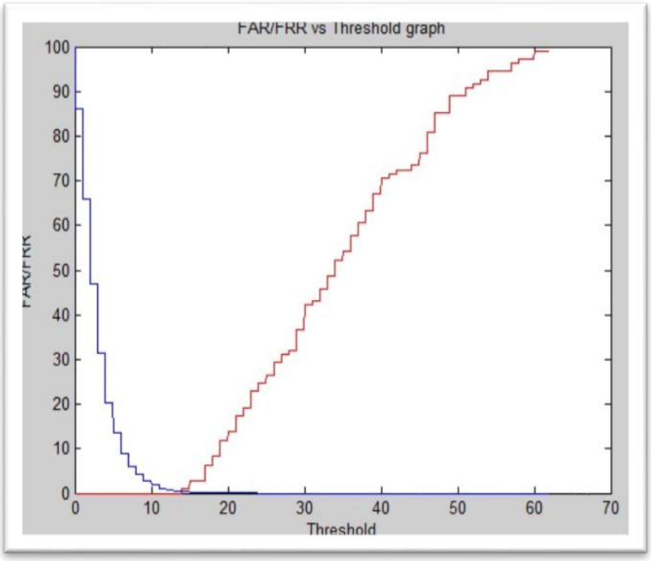


Fig 5.5: FAR/FRR vs. Threshold curve for face profile

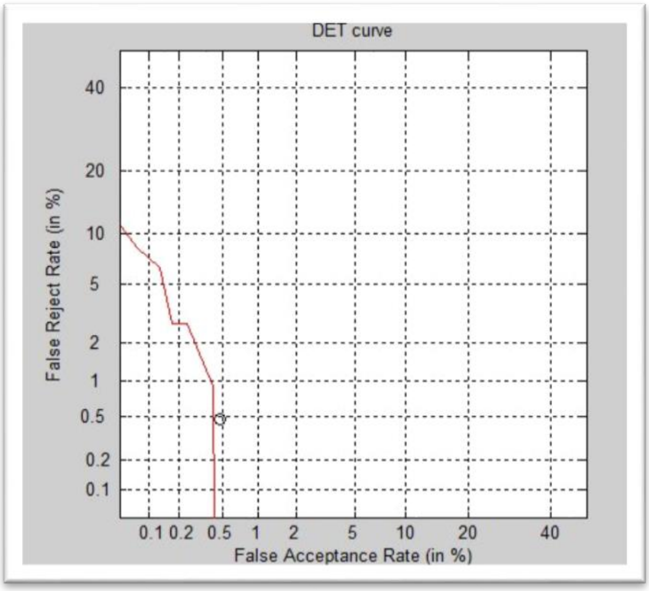


Fig 5.6: DET curve for face profile

5.3 After Fusion

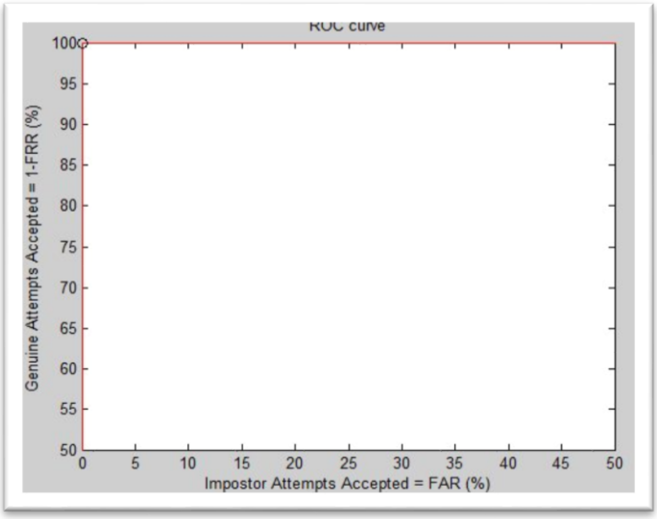


Fig 5.7: ROC curve for sum

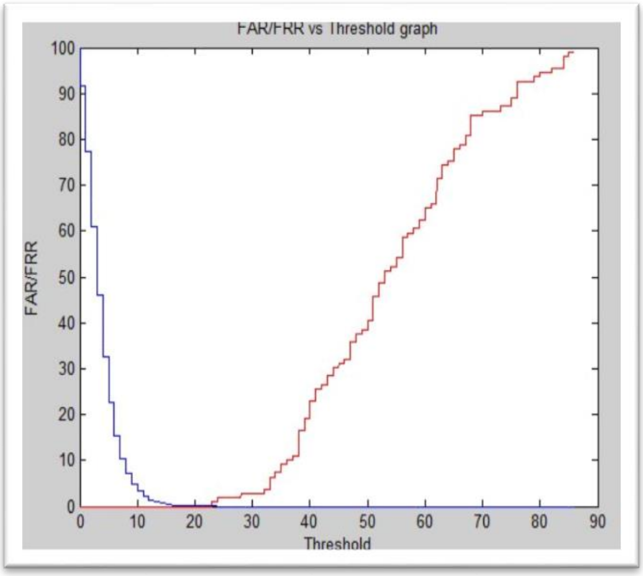


Fig 5.8: FAR/FRR vs. Threshold curve for sum

6. RESULT

A. Ear images:

FAR: 0.7985

FRR: 0

EER: 0.3993

Accuracy = 99.6007%

B. Face portion

FAR: 0.5607

FRR: 0

EER: 0.6626

Accuracy = 99.3374%

C. After fusion

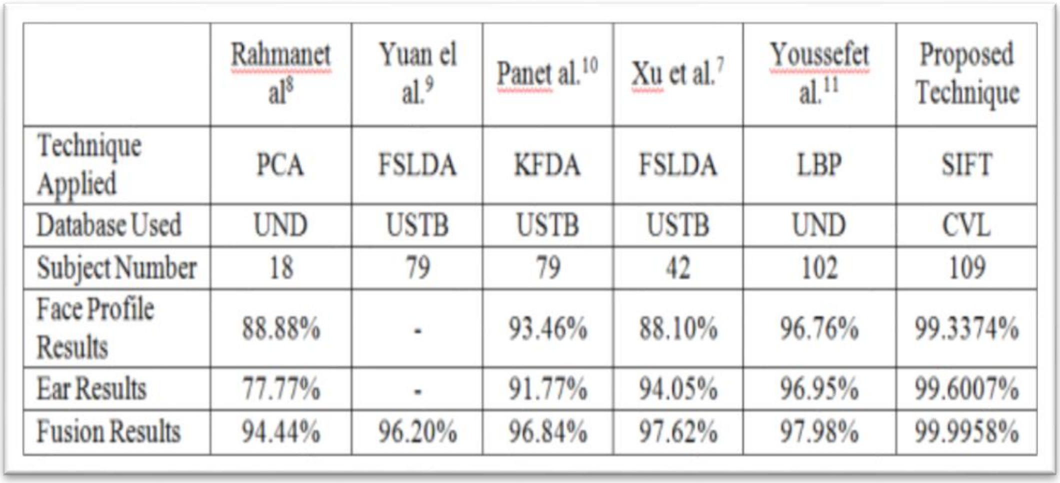
FAR: 0.0085

FRR: 0

EER: 0.0042

Accuracy = 99.9958%

Table 6.1: Comparison between various techniques



	Rahmanet al[8]	Yuan el al.[9]	Panet al.[10]	Xu et al.[7]	Youssefet al.[11]	Proposed Technique
Technique Applied	PCA	FSLDA	KFDA	FSLDA	LBP	SIFT
Database Used	UND	USTB	USTB	USTB	UND	CVL
Subject Number	18	79	79	42	102	109
Face Profile Results	88.88%	-	93.46%	88.10%	96.76%	99.3374%
Ear Results	77.77%	-	91.77%	94.05%	96.95%	99.6007%
Fusion Results	94.44%	96.20%	96.84%	97.62%	97.98%	99.9958%

7. CONCLUSION

In this project a new multi-biometric system has been proposed mainly for the surveillance system whereby the side face is used to extract the face-profile and ear. In this work, the process of extraction has been done manually, however this could be automated in future using techniques such as template matching. The SIFT algorithm is the best feature extraction algorithm which could be used in biometric security as it gives a recognition accuracy of around 99%. The SIFT algorithm would provide similar results independent of the database being used. The proposed multi-biometric system gives higher recognition accuracy on combining the unimodal biometric traits of face-profile and ear using simple summation technique of the matching scores.

Another important thing to note is the value of FRR which is zero for both the unimodal and multimodal trait. This implies that using the SIFT algorithm completely removes the possibility of accepting an imposter. However the value of FAR is not exactly zero, so there is even a small possibility that a genuine user may be rejected. The value of FRR makes the proposed system perfect for use in surveillance system. As the objective in surveillance system is to correctly identify an individual whose records are stored.

8. CODE

If we have access to Matlab, scripts are provided for loading SIFT features and finding matches between images. These were tested under Matlab Version 7 and do not require the image processing toolbox.

Run Matlab in the current directory and execute the following commands. The "sift" command calls the appropriate binary to extract SIFT features (under Linux or Windows) and returns them in matrix form. Use "showkeys" to display the keypoints superimposed on the image:

```
[image, descrips, locs] = sift('scene.pgm');
showkeys(image, locs);
```

The "match" command is given two image file names. It extracts SIFT features from each image, matches the features between the two images, and displays the results.

```
match('scene.pgm','book.pgm');
```

The result shows the two input images next to each other, with lines connecting the matching locations. Most of the matches should be correct (as can be roughly judged by the fact that they select the correct object in a cluttered image), but there will be a few false outliers that could be removed by enforcing viewpoint consistency constraints.

We can also try matching other images:

```
match('scene.pgm','box.pgm');
match('scene.pgm','basmati.pgm');
```

For more details, see the comments in the Matlab scripts: sift.m, showkeys.m, and match.m.

Acknowledgments: The Matlab script for loading SIFT features is based on one provided by D. Alvaro and J.J. Guerrer

runme.m

```
D=[];
for i=1:109
   for j=1:109
     m=matching(i,j);
     D(i,j)=m;
   end
end

dlmwrite('output_sideface.txt', D, ' ');
type output_sideface.txt;
```

matching.m

```
function n = matching( first , second )
%matching Summary of this function goes here
% Detailed explanation goes here
    ext = '.jpg';
    str1= num2str(first); %first converted to string
    str2= num2str(second); %second converted to string
    first1= strcat(str1,ext);
    second2= strcat(str2,ext);
    n=  match(fullfile('side  face',first1),fullfile('side
face',second2));
end
```

match.m

```
% num = match(image1, image2)
%
%  This  function  reads  two  images,  finds  their  SIFT
features, and displays lines connecting the matched    %
```

```
keypoints.  A match is accepted only if its distance is
less than distRatio times the distance to the          %
second closest match. It returns the number of matches
displayed. Example:                                    %
match('scene.pgm','book.pgm');


function num = match(image1, image2)


% Find SIFT keypoints for each image

[im1, des1, loc1] = sift(image1);

[im2, des2, loc2] = sift(image2);


% For efficiency in Matlab, it is cheaper to compute dot
products between

%  unit vectors rather than Euclidean distances.  Note that
the ratio of

%  angles (acos of dot products of unit vectors) is a close
approximation

%  to the ratio of Euclidean distances for small angles.

%

% distRatio: Only keep matches in which the ratio of vector
angles from the

%    nearest to second nearest neighbor is less than
distRatio.

distRatio = 0.6;


% For each descriptor in the first image, select its match
to second image.

des2t = des2';                          % Precompute matrix
transpose

for i = 1 : size(des1,1)

   dotprods = des1(i,:) * des2t;        % Computes vector
of dot products

   [vals,indx] = sort(acos(dotprods));   % Take inverse
cosine and sort results
```

```
   % Check if nearest neighbor has angle less than distRatio times 2nd.
   if (vals(1) < distRatio * vals(2))
      match(i) = indx(1);
   else
      match(i) = 0;
   end
end



% Create a new image showing the two images side by side.
im3 = appendimages(im1,im2);

% Show a figure with lines joining the accepted matches.
figure('Position', [100 100 size(im3,2) size(im3,1)]);
colormap('gray');
imagesc(im3);

hold on;
cols1 = size(im1,2);
for i = 1: size(des1,1)
  if (match(i) > 0)
    line([loc1(i,2) loc2(match(i),2)+cols1], ...
         [loc1(i,1) loc2(match(i),1)], 'Color', 'c');
  end
end
hold off;

num = sum(match > 0);
fprintf('Found %d matches.\n', num);
```

❖ sift.m

```
% [image, descriptors, locs] = sift(imageFile)
%
% This function reads an image and returns its SIFT keypoints.
%   Input parameters:
%     imageFile: the file name for the image.
%
%   Returned:
%     image: the image array in double format
%     descriptors: a K-by-128 matrix, where each row gives an invariant
%         descriptor for one of the K keypoints.  The descriptor is a vector
%         of 128 values normalized to unit length.
%     locs: K-by-4 matrix, in which each row has the 4 values for a
%         keypoint location (row, column, scale, orientation).  The
%         orientation is in the range [-PI, PI] radians.
%
% Credits: Thanks for initial version of this program to D. Alvaro and
%          J.J. Guerrero, Universidad de Zaragoza (modified by D. Lowe)

function [image, descriptors, locs] = sift(imageFile)

% Load image
image = imread(imageFile);

% If we have the Image Processing Toolbox, we can uncomment the following
%   lines to allow input of color images, which will be
converted to grayscale.
%if isrgb(image)
    image = rgb2gray(image);
%end

[rows, cols] = size(image);

% Convert into PGM imagefile, readable by "keypoints"
executable
f = fopen('tmp.pgm', 'w');
if f == -1
    error('Could not create file tmp.pgm.');
end
fprintf(f, 'P5\n%d\n%d\n255\n', cols, rows);
fwrite(f, image', 'uint8');
fclose(f);

% Call keypoints executable
if isunix
    command = '!./sift ';
else
    command = '!siftWin32 ';
end
command = [command ' <tmp.pgm >tmp.key'];
eval(command);

% Open tmp.key and check its header
g = fopen('tmp.key', 'r');
if g == -1
    error('Could not open file tmp.key.');
end
[header, count] = fscanf(g, '%d %d', [1 2]);
```

```
if count ~= 2
    error('Invalid keypoint file beginning.');
end
num = header(1);
len = header(2);
if len ~= 128
    error('Keypoint descriptor length invalid (should be
128).');
end

% Creates the two output matrices (use known size for
efficiency)
locs = double(zeros(num, 4));
descriptors = double(zeros(num, 128));

% Parse tmp.key
for i = 1:num
    [vector, count] = fscanf(g, '%f %f %f %f', [1 4]); %row
col scale ori
    if count ~= 4
        error('Invalid keypoint file format');
    end
    locs(i, :) = vector(1, :);

    [descrip, count] = fscanf(g, '%d', [1 len]);
    if (count ~= 128)
        error('Invalid keypoint file value.');
    end
    % Normalize each input vector to unit length
    descrip = descrip / sqrt(sum(descrip.^2));
    descriptors(i, :) = descrip(1, :);
end
fclose(g);
```

9. REFERENCES

[1]. Wang, Yunhong, Tieniu Tan, and Anil K. Jain. “Combining face and iris biometrics for identity verification”. Audio-and Video Based Biometric Person Authentication. Springer Berlin Heidelberg, 2003.

[2]. Karanwal, Shekhar, Davendra Kumar, and RohitMaurya. "Fusion of fingerprint and face by using DWT and SIFT." Int J ComputAppl 2.5 (2010): 0975-8887.

[3]. Lowe, David G. "Distinctive image features from scale-invariant key-points. “International journal of computer vision 60.2 (2004): 91 -110.

[4]. Bagal, Ms VL, N. B. Sambre, and P. Malathi. "Identification of Person by fusion and using Scale Invariant Feature Transform."

[5]. Verma, Shalini, and R. K. Singh. "Multimodal Biometrics Information Fusion for Efficient Recognition using Weighted Method."

[6]. Cummings, Alastair H., Mark S. Nixon, and John N. Carter. "A novel ray analogy for enrolment of ear biometrics." Biometrics:

[7]. Xu, X. and Mu, Z.-C., “Multimodal recognition based on fusion of ear and profile face,” in [Proc. of the 4th International Conference on Image and Graphics ICIG], 598–603 (2007).

[8]. Rahman,M.M.Ishikawa ,Proposing a passive biometric system for robotic vision,” in [Proc. of the 10thInternational Symposium on Artificial Life and Robotics (AROB)], (Feb 2005).

[9]. Yuan, L., Mu, Z.-C., and Liu, Y., “Multimodal recognition using face profile and ear,” in [Proc. of the IEEE International Symposium on Systems and Control in Aerospace and Astronautics ISSCAA], 887–891 (2006).

[10]. Pan, X., Cao, Y., Xu, X., Lu, Y., and Zhao, Y., “Ear and face based multimodal recognition based on KFDA,” in [Proc. of the International Conference on Audio, Language and Image Processing ICALIP], 965–969 (2008).

[11]. Youssef, Iman S., et al. "Multimodal biometrics system based on face profile and ear." SPIE Defence + Security. International Society for Optics and Photonics, 2014.

10. BIBLIOGRAPHY

Akash Pal is a student of final year B.Tech in Computer Science & Engineering Department in JIS College of Engineering, West Bengal, India. He has attended various national and international conferences. He has been awarded as the best researcher by the Computer Science & Engineering Department in JIS College of Engineering. His research interest includes image processing, biometric security, ecommerce security, and robotics

Avinandan Sau is a student of final year B.Tech in Computer Science & Engineering Department in JIS College of Engineering, West Bengal, India. His research interest includes image processing, biometric security, cyber security, and robotics

Debolina Das is a student of final year B.Tech in Computer Science & Engineering Department in JIS College of Engineering, West Bengal, India. Her research interest includes Image Processing, Cyber Security

Sukanta Sharma is a student of final year B.Tech in Computer Science & Engineering Department in JIS College of Engineering, West Bengal, India. His research interest includes image processing, biometric security.