FACIAL RECOGNITION SYSTEM

Submitted in partial fulfilment of the Degree of

Bachelor of Technology

May – 2012

Name of Students - Akshima Arora (081052)
Swena Gupta (081090)
Vyom Mathur (081103)

Name of supervisor - Dr. S.V. Bhushan

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

CERTIFICATE

This is to certify that project report entitled "Facial Recognition System", submitted by Akshima, Swena and Vyom in partial fulfillment for the award of degree of Bachelor of Technology in Electronics and Communication Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Supervisor's Name : Dr. S.V. Bhushan

Designation: Head of Department

ACKNOWLEDGEMENT

"EXPRESSION OF FEELINGS BY WORDS MAKES THEM LESS SIGNIFICANT WHEN IT COMES TO MAKE STATEMENT OF GRATITUDE"

We think the most pleasant and satisfying aspect of writing project report is the opportunity to thank those who have contributed to it. Although the expression of gratitude always remains incomplete and inadequate no matter how extensive it is. Firstly we would like to express our gratitude to **Brig. (Retd.) Balbir Singh,** Director, Jaypee University of Information Technology.

We would like to acknowledge our profound gratitude to **Dr. S.V. Bhushan,** HOD, Electronics Department, Jaypee University of Information Technology, for his supervision, guidance, patience and care. He left no stone unturned to make our project a great learning experience. He is a kind of mentor who not only assigns tasks but also makes it clear that there should be result with learning to make it better. He has always been kind enough to extend his personal attention and scholarly advice while preparing the project report.

Akshima Arora
Swena Gupta
Vyom Mathur

TALBLE OF CONTENTS

List Of Figures

SUMMARY

In today's world where security and protection is of prime importance, we have developed a software by which physical presence of an individual can be verified based by the detection of his facial features.

The software can be used in attendance systems, access in the important areas of an institution, real time detection of the miscreants in proximity of the software. In the contemporary world where the number of mishaps and miscreants is surging, the software can be of great help in curbing them. The software exploits the uniqueness of certain biometric features.

The software has three layers:

1. **Database:** Faces of the people will be entered by using cameras, web cameras or any other equipment by which a photograph of a person can be taken. The photograph will be stored inside the database, which can also be updated from time to time.
2. **Feature extraction:** The highlighting features of the face of a person will be extracted using eigen values and eigen vectors.
3. **Tallying:** The extracted face will be tallied with the faces in the database. If the extracted face matches with a face recorded in the database, then the person's presence will be verified.

If the software finds that the face extracted matches with a face in the database, then that person can be marked present, granted access or the software will inform the operator of the presence of the miscreant.

The software can also be clubbed with the fingerprint recognising biometric to provide two layer securities. The exploitation of biometric features also removes the use of fake masks or the copied fingerprints where only fingerprint biometric is used.

CHAPTER-1

INTRODUCTION

1.1 Introduction:

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Face recognition technology may solve this problem since a face is undeniably connected to its owner expect in the case of identical twins. It is non-transferable.

A **facial recognition system** is computer application software by which physical presence of an individual can be verified based by the detection of his facial features.

Geometric models were used as initial parameters in facial recognition. But these days facial recognition uses complex and higher mathematical representations and matching processes.

In previous couple of decades where security issues rose, technology had to stand tall to meet the demands of the end users. For the technology to be worldwide acceptable it must be simple and must be able to protect the privacy of its users. This grabbed the attention of the scientists towards Biometrics.

Face recognition is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. The idea behind authentication through face recognition is that no two faces are alike. As face has both uniqueness and permanence, they can be used as a trusted form of identification.

Facial recognition can also be used in ATM machines. Instead of using bank card, the ATM would capture an image of the face and would proceed with banking if the face matches with the face in the database.

1.2 What is Face Recognition ?

Your face Your Identity

Face recognition technology is the least intrusive and fastest biometric technology[1]. It works with the most obvious individual identifier – the human face.

Instead of requiring people to place their hand on a reader or precisely position their eyes in front of a scanner, Face Recognition systems silently take pictures of people's faces as they enter a defined area. There is no intrusion or delay, and in most cases the subjects are entirely unaware of the process. They do not feel "under surveillance" or that their privacy has been invaded.

FRS Technology

Facial Recognition analyzes the characteristics of a person's face images input through a digital video camera. It measures the overall facial structure. These measurements are retained in a database and used for comparisons when a user stands before the camera. This biometric has been widely and perhaps wildly, touted as a fantastic system for recognizing potential threats. (Whether terrorist, scam artist or known criminal)but so far has been unproven in high-level usage. It is currently used only in verification systems with a good deal of success.

Every face has numerous, distinguishable landmarks and the different peaks and valleys- that make up one’s facial characteristics unique.

How it Works [2]

The following four-stage process illustrates the way biometric systems operate:

Capture - : Physical or behavioral sample is captured by the system during enrollment

Extraction - Unique data is extracted from the sample and a template is created

Comparison - The template is then compared with a new sample

Matching - The system then decides if the features extracted from the new sample are matching or not.

User faces the camera, standing about two feet from it. The system will locate the user's face and perform matches against the claimed identity or the facial database. It is possible that the user may need to move and re-attempt the verification based on his facial position. The system usually comes to a decision in less than 5 seconds.

Use

Currently gaining support as a potential tool for averting terrorist crimes, facial recognition system is already in use in many law enforcement areas. Software has already been developed for computer networks and automated bank tellers that use facial recognition for user verification purposes.

Evaluation

One of the strongest positive aspects of facial Recognition is that it is non-invasive. Verification or identification can be accomplished from a distance of two feet or more without requiring the user to wait for a longer period of time or do anything more than look at the camera.

Face Recognition is also very difficult to dupe. It works by comparing facial landmarks - specific proportions and angles of defined facial features - which cannot easily be concealed by beards, eyeglasses or makeup.

The ideal solution

All of these makes face recognition ideal for high traffic areas open to the general public, such as:-

- Airports & Railway Stations
- Corporate
- Cash-Points
- Stadiums
- Public Transportation
- Financial Institutions
- Government Offices

1.3 Block Diagram:

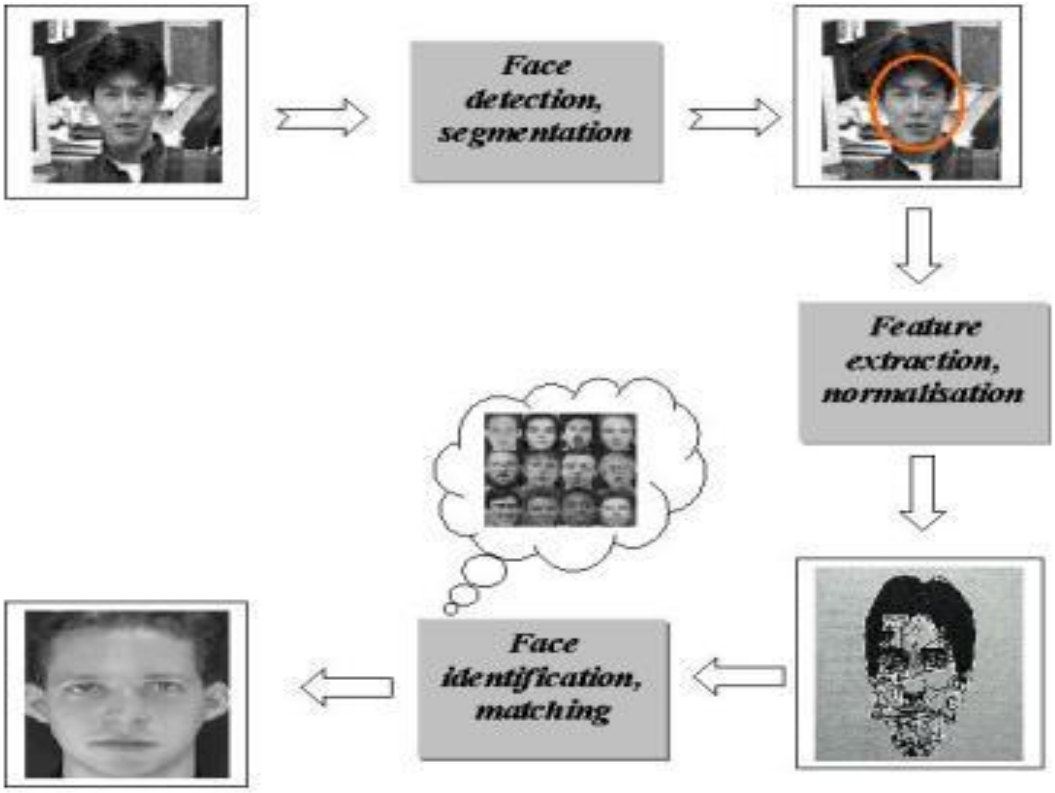


Fig 1.1 Block Diagram for Facial Recognition.[3]

1.4 Objective:

The objective of our project is to recognise a person's face and then verify it against a pre registered database to authenticate an individual for access to a system thereby ensuring security of the system.

Geometric models were used as initial parameters in facial recognition. But these days facial recognition uses complex and higher mathematical representations and matching processes.

The database creation is the first stage; it includes capturing image of a candidate from a live video.

The recognition stage is the second stage; it includes feature extraction, where important information for discrimination is saved, and the matching, where the recognition result is given with the aid of a face database. Face recognition can be used for both verification and identification.

We have developed a software system which can be used to recognize face for various purposes.

1.5 Advantages:

- It is natural, easy to use and can be used in various small scale and large scale institutions.
- The biometric concept can be used with photograph data-bases, videotape, or other image sources.
- Facial recognition can be used in Illegal immigrant detection, Passport authentication.
- Face recognition can be used for identification of miscreants in a crowd, in real time.

Fig 1.2 Real Time Face Recognition [4]

1.6 Robustness and Frauds:

Verification or authentication is the simplest task for a FRS. An individual with a pre-existing relationship with an institution (and therefore already enrolled in the reference database or gallery) presents his or her biometric characteristics (face or probe image) to the system, claiming to be in the reference database or gallery (i.e. claiming to be a legitimate identity). The system must then attempt to match the probe image with the particular, claimed template in the reference database. This is a one-to-one matching task since the system does not need to check every record in the database but only that which corresponds to the claimed identity (using some form of identifier such as an employee number to access the record in the reference database). There are two possible outcomes: (1) the person is not recognized or (2) the person is recognized. If the person is not recognized (i.e., the identity is not verified) it might be because the person is an imposter (i.e., is making an illegitimate identity claim) or because the system made a mistake (this mistake is refer red to as a false reject). The system may also make a mistake in accepting a claim when it is in fact false (this is refer red to as a false accept).

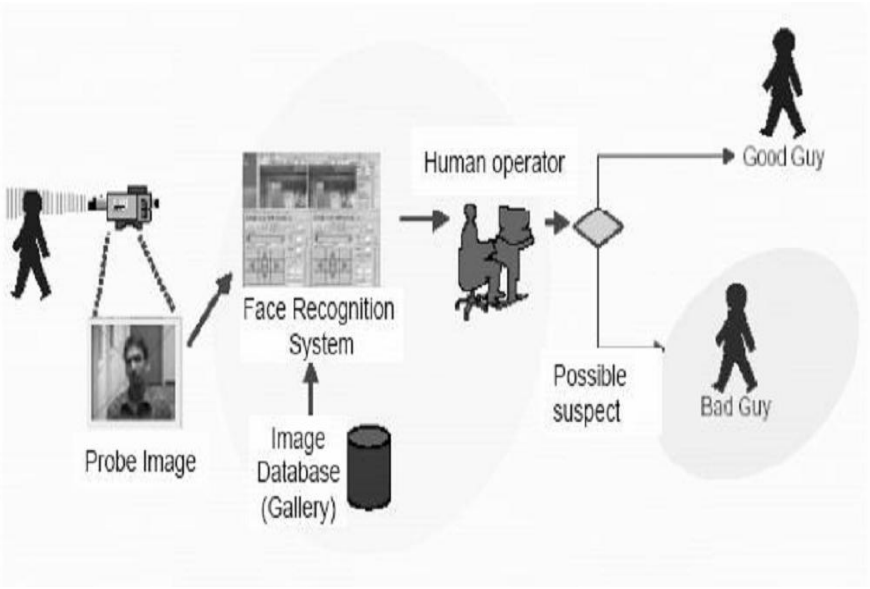


Fig 1.3 Block diagram of possible outcomes[5]

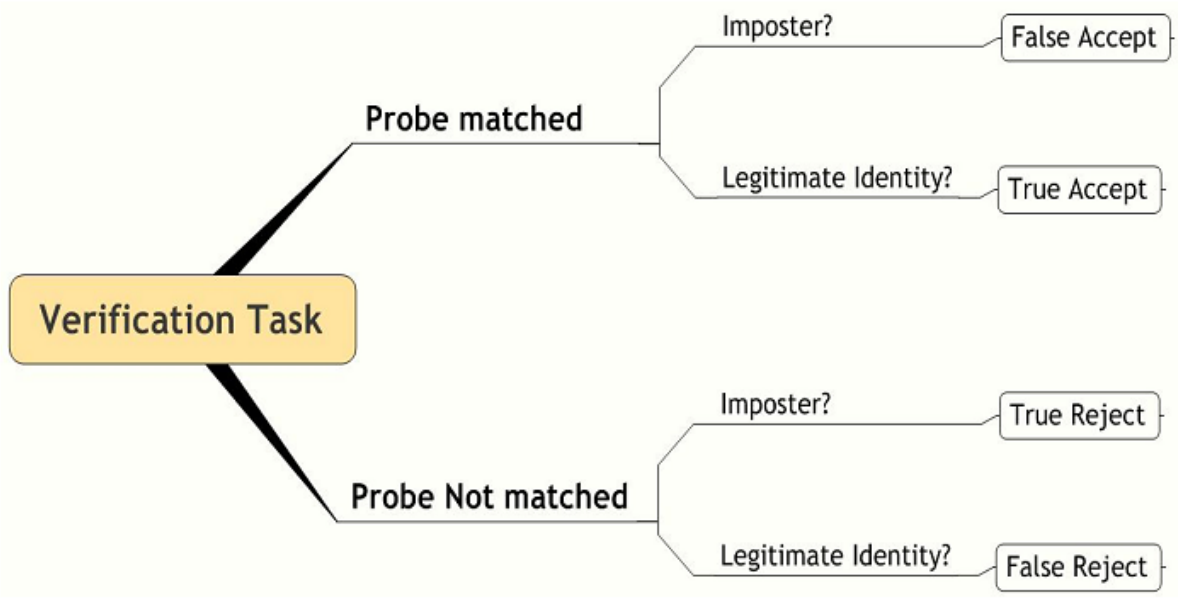


Fig 1.4 Verification Task

1.7 Why we choose face recognition over other biometric?

There are number reasons to choose face recognition. This includes the following

a. It requires no physical interaction on behalf of the user.

b. It is accurate and allows for high enrolment and verification rates.

c. It does not require an expert to interpret the comparison result.

d. It can use your existing hardware infrastructure, existing cameras and image capture Devices will work with no problems

e. It is the only biometric that allow you to perform passive identification in a one to many environments (e.g.: identifying a terrorist in a busy Airport terminal)

1.8 Software Used:

- **MATLAB 7.1**

MATLAB (**mat**rix **lab**oratory) is a numerical computing software which allows matrix manipulations, plotting of functions and data, implementation of algorithms. Most MATLAB functions can accept matrices and will apply themselves to each element when applied on a matrix so can be used in image processing.

Chapter 2

Face Recognition Techniques

2.1 Some Basic Existing Techniques:

- **Traditional[6]**

Some facial recognition algorithms identify faces by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face detection. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation.

Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features, or photometric, which is a statistical approach that distills an image into values and comparing the values with templates to eliminate variances.

Popular recognition algorithms include

- ❖ Principal Component Analysis using eigenfaces,
- ❖ Linear Discriminant Analysis
- ❖ Elastic Bunch Graph Matching

Fig 2.1 Traditional technique of recognition [7]

- **3 Dimensional recognition[8]**

A newly emerging trend, claimed to achieve improved accuracies, is three-dimensional face recognition. This technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin.

One advantage of 3D facial recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view. Three-dimensional data points from a face vastly improve the precision of facial recognition. 3D research is enhanced by the development of sophisticated sensors that do a better job of capturing 3D face imagery. The sensors work by projecting structured light onto the face. Up to a dozen or more of these image sensors can be placed on the same CMOS chip -- each sensor captures a different part of the spectrum.

Even a perfect 3D matching technique could be sensitive to expressions. For that goal a group at the "Technion" applied tools from metric geometry to treat expressions as isometries. A company called Vision Access created a firm solution for 3D facial recognition. The company was later acquired by the biometric access company "Bioscrypt Inc." which developed a version known as 3D Fast Pass.

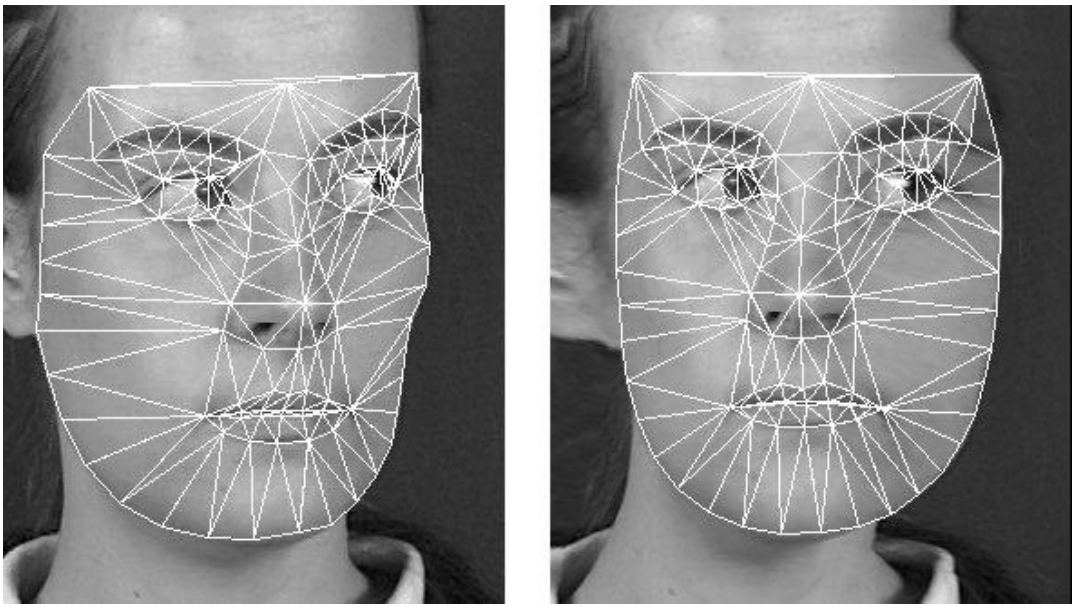


Fig 2.2 3-D technique[9]

- **Skin texture analysis**[10]

Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person's skin into a mathematical space.

Tests have shown that with the addition of skin texture analysis, performance in recognizing faces can increase 20 to 25 percent.

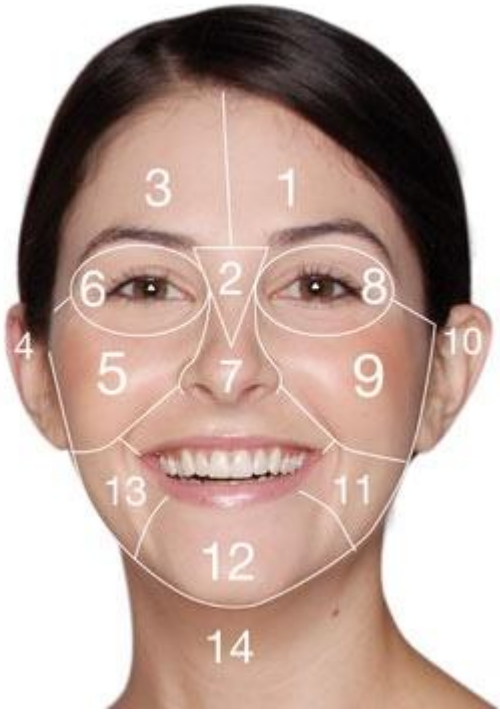


Fig 2.3 Skin texture analysis [11]

- **Discrete Cosine Transform**

A discrete cosine transform (DCT)[12] expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as described below, fewer are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions. In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real

and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT"; its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transforms (DST), which is equivalent to a DFT of real and odd functions, and the modified discrete cosine transforms (MDCT), which is based on a DCT of overlapping data.

CHAPTER – 3

FACE RECOGNITION

3.1 Introduction

Facial recognition research and FRT (Facial Recognition Technique) is a subfield in a larger field of pattern recognition research and technology. Pattern recognition technology uses statistical techniques to detect and extract patterns from data in order to match it with patterns stored in a database. The data upon which the recognition system works (such as a photo of a face) is no more than a set of discernable pixel-level patterns for the system, that is, the patter n recognition system does not perceive meaningful "faces" as a human would understand them. Nevertheless, it is very important for these systems to be able to locate or detect a face in a field of vision so that it is only the image pattern of the face (and not the background "noise") that is processed and analyzed.

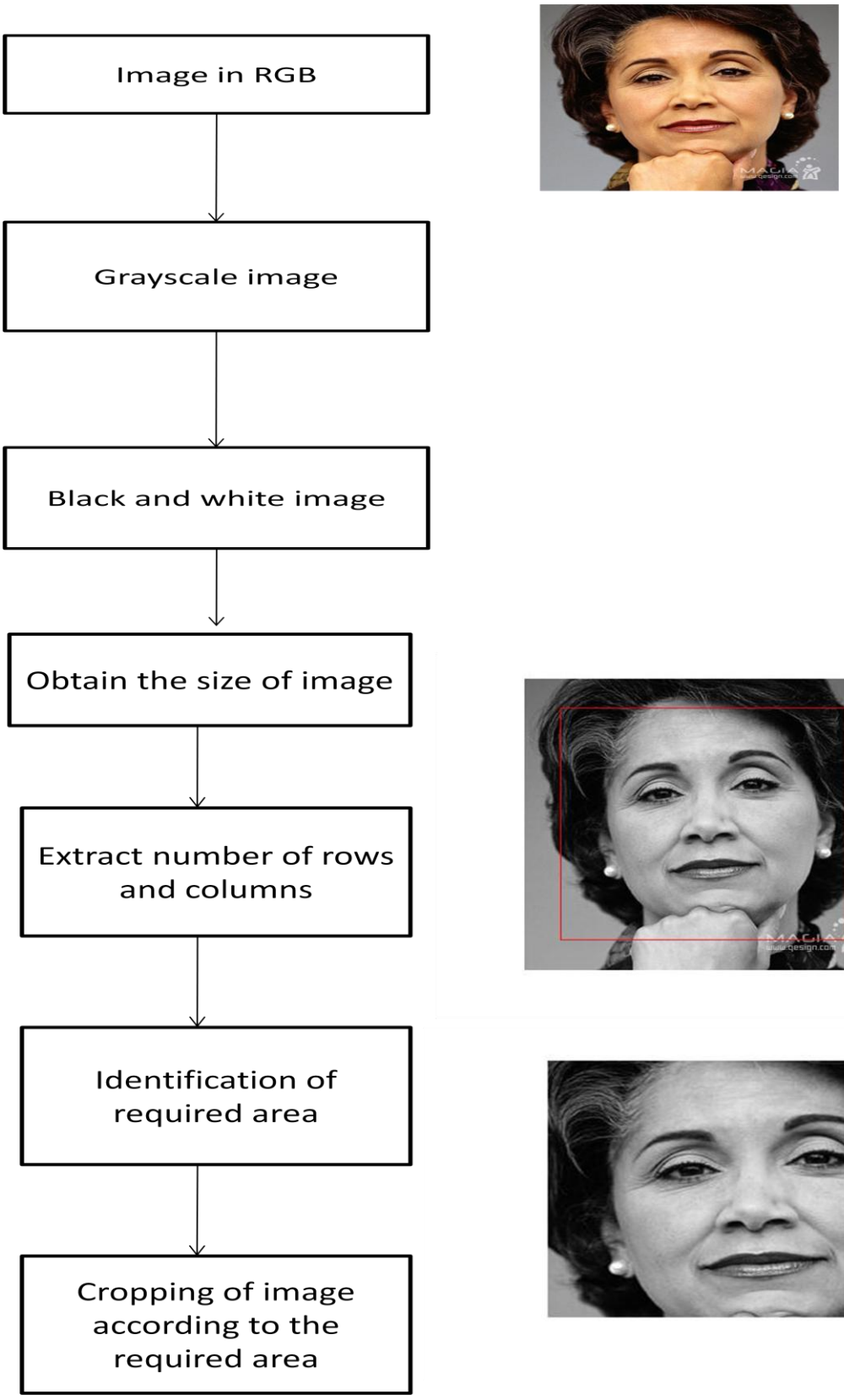
The first step in the facial recognition process is the capturing of a face image, also known as the probe image. This would normally be done using a still or video camera. In principle, the capturing of the face image can be done with or without the knowledge (or cooperation) of the subject. This is indeed one of the most attractive features of FRT. The effectiveness of the whole system is highly dependent on the quality and characteristics of the captured face image. The process begins with facial feature extraction from the larger image. The system will, to the extent possible, "normalize" (or standardize) the probe image so that it is in the same format (size, rotation, etc.) as the images in the database. The normalized face image is then passed to the recognition software.

3.2 Initial approach

(1). The essential thought behind the algorithm was that local object appearance and shape within an image can be described by the distribution of intensity gradients.

Keeping the same concept in mind we developed an algorithm for detection of the face of a person.

Algorithm:



Results:

Fig 3.1 Result of face detection

Reason of Failure:

Since this approach was completely based on the intensity gradients of an image, it did not always give accurate results in the absence of proper light or in different background.

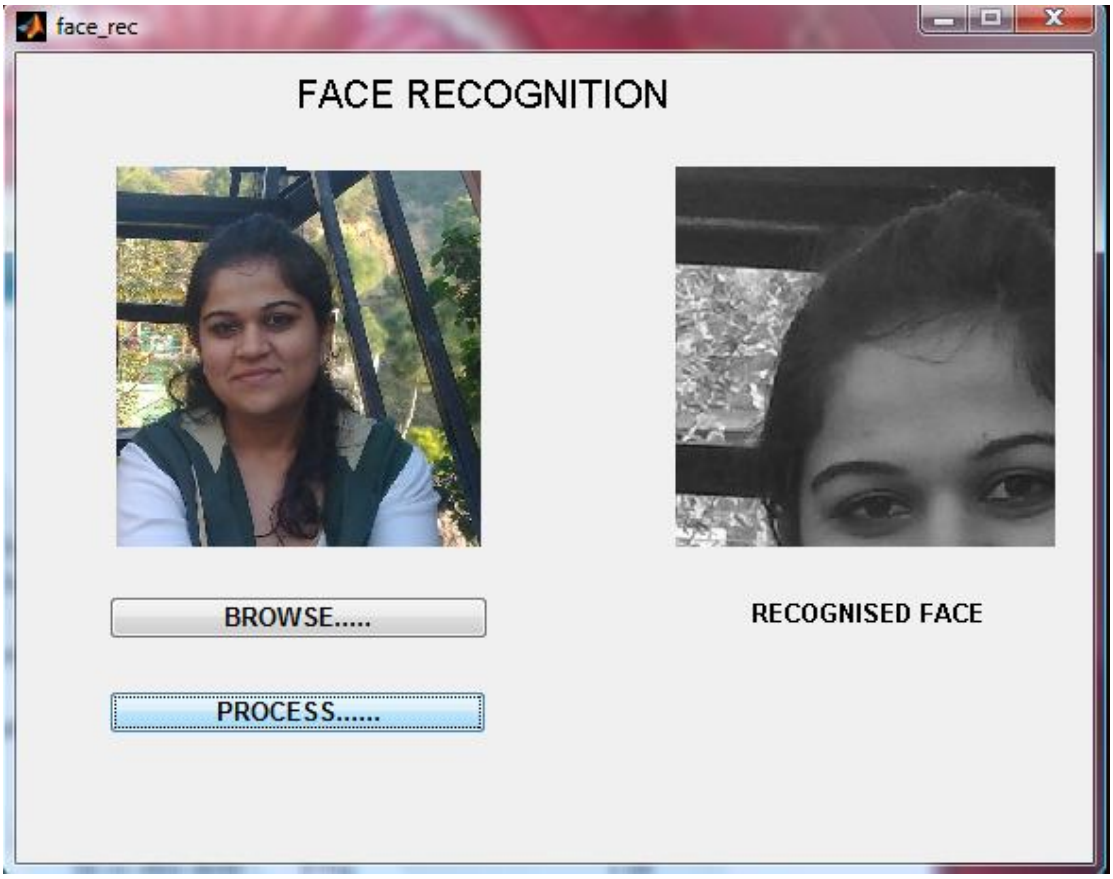


Fig 3.2 Failed result

(2). We also worked on a technique based on geometrical pattern of a face. In this we were to identify various points on the face and calculate distance between them. This distance is unique for every person.

The approach was complex and time consuming as locating all the distinct points on a face and calculating distance between them would have required a complex code which would take a lot of time to process making the recognition slow.

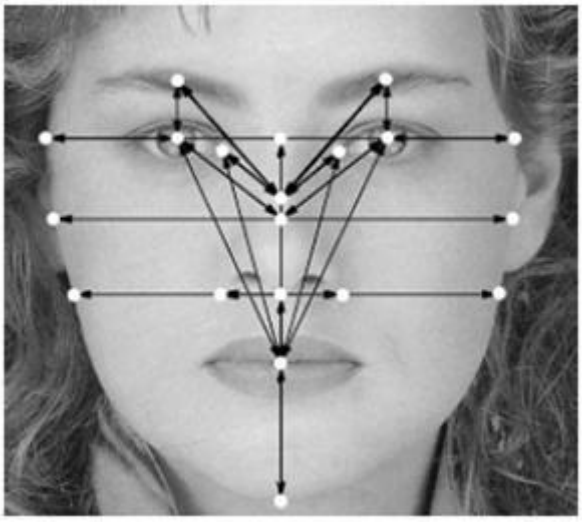


Fig 3.3 Geometrical aspects [13]

3.3 Current approach:

Eigenface-based facial recognition

The task of facial recognition is discriminating input signals (image data) into several classes (persons). The input signals are highly noisy (e.g. the noise is caused by differing lighting conditions, pose etc.), yet the input images are not completely random and in spite of their differences there are patterns which occur in any input signal. Such patterns, which can be observed in all signals could be - in the domain of facial recognition - the presence of some objects (eyes, nose, mouth) in any face as well as relative distances between these objects. These characteristic features are called eigenfaces in the facial recognition domain (or principal components generally). They can be extracted out of original image data by means of a mathematical tool called Principal Component Analysis (PCA).[14]

By means of PCA one can transform each original image of the training set into a corresponding eigenface. An important feature of PCA is that one can reconstruct any original image from the training set by combining the eigenfaces.[15] Remember that eigenfaces are nothing less than characteristic features of the faces. Therefore one could say that the original face image can be reconstructed from eigenfaces if one

adds up all the eigenfaces (features) in the right proportion. Each eigenface represents only certain features of the face, which may or may not be present in the original image. If the feature is present in the original image to a higher degree, the share of the corresponding eigenface in the "sum" of the eigenfaces should be greater. If, contrary, the particular feature is not (or almost not) present in the original image, then the corresponding eigenface should contribute a smaller (or not at all) part to the sum of eigenfaces. So, in order to reconstruct the original image from the eigenfaces, one has to build a kind of weighted sum of all eigenfaces. That is, the reconstructed original image is equal to a sum of all eigenfaces, with each eigenface having a certain weight. This weight specifies, to what degree the specific feature (eigenface) is present in the original image.

If one uses all the eigenfaces extracted from original images, one can reconstruct the original images from the eigenfaces exactly. But one can also use only a part of the eigenfaces. Then the reconstructed image is an approximation of the original image. However, one can ensure that losses due to omitting some of the eigenfaces can be minimized. This happens by choosing only the most important features (eigenfaces). Omission of eigenfaces is necessary due to scarcity of computational resources. How does this relate to facial recognition? The clue is that it is possible not only to extract the face from eigenfaces given a set of weights, but also to go the opposite way. This opposite way would be to extract the weights from eigenfaces and the face to be recognized. These weights tell nothing less, as the amount by which the face in question differs from "typical" faces represented by the eigenfaces. Therefore, using this weights one can determine two important things:

1. Determine, if the image in question is a face at all. In the case the weights of the image differ too much from the weights of face images (i.e. images, from which we know for sure that they are faces), the image probably is not a face.
2. Similar faces (images) possess similar features (eigenfaces) to similar degrees (weights). If one extracts weights from all the images available, the images could be grouped to clusters. That is, all images having similar weights are likely to be similar faces.

3.3 Algorithm

1. Database creation

1. • asks the user for input image folder number
2. • initialise the web cam
3. • live video is started
4. • a new folder is created in the current directory with name same as of folder number concatenated with 's'.
5. • ten images of each subject are taken to improve accuracy
6. • the images are saved in their respective folder and converted into gray scale index simultaneously.
7. • the saved images are resized into a standard size.

2. Face recognition

1. •the database created is first loaded
2. • webcam is initialised
3. •a snapshot of the candidate whose face is to be recognised is taken
4. •the image taken is converted into gray scale and resized in same size as those of the images in the database.
5. •the average of database images is taken for accuracy and this mean is subtracted from the image.
6. •for each image correlation matrix is calculated.
7. •eigenvectors of each correlation matrix is calculated.
8. • the eignevectors corresponding to the 10 largest eigenvalues are picked.
9. •the signature(highlighting features or largest eigenvectors) for each image is calculated.
10. •correlation matrix and largest eigenvectors are calculated for current image.
11. •the highlighting features of current image and database images are compared.
12. •the database image with minimum variations from the current image is displayed as the recognised image
13. •if no such image is found in the database, a message 'Not found' is displayed.

3.4 Code

1.Database creation:

```
i= input('which folder number    :     ', 's');
vid=videoinput('winvideo',1,'YUY2_160x120');
cd('att_faces');
  mkdir(strcat('s',num2str(i)));
  cd(strcat('s',num2str(i)));
  for j=1:10
     b=getsnapshot(vid);
     a=ycbcr2rgb(b);
     a= rgb2gray(a);
     a = imresize(a, [112 92]);
     imwrite(a,strcat(num2str(j),'.pgm'));
  end
```

2.Face Recognition:

```
%% Loading the database into matrix v
clear;
clc;
w=load_database();
warning ('off');
vid=videoinput('winvideo',1,'YUY2_160x120');
 b=  getsnapshot(vid);
 a=ycbcr2rgb(b);
 a= rgb2gray(a);
 a = imresize(a, [112 92]);
ri=round(400*rand(1,1));
r= reshape(a,size(a,1)*size(a,2),1);
% r contains the image we later on will use to test the algorithm
v=w;
```

```
N=70;                                   % Number of signatures used for each image.

%% Subtracting the mean from v
O=uint8(ones(1,size(v,2)));
m=uint8(mean(v,2));                     % m is the maen of all images.
vzm=v-uint8(single(m)*single(O));   % vzm is v with the mean removed.

%% Calculating eignevectors of the correlation matrix
L=single(vzm)'*single(vzm);
[V,D]=eig(L);
V=single(vzm)*V;
V=V(:,end:-1:end-(N-1));
% Pick the eignevectors corresponding to the 10 largest eigenvalues.


%% Calculating the signature for each image
cv=zeros(size(v,2),N);
for i=1:size(v,2);
   cv(i,:)=single(vzm(:,i))'*V;    % Each row in cv is the signature for one image.
End

%% Recognition
%  Now, we run the algorithm and see if we can correctly recognize the face.
subplot(121);
imshow(reshape(r,112,92));title('Looking for ...','FontWeight', 'bold', 'Fontsize',
16,'color','red')

subplot(122);
p=r-m;                          % Subtract the mean
s=single(p)'*V;
z=[ ];
for i=1:size(v,2)
   z=[z,norm(cv(i,:)-s,2)];
   if(rem(i,20)==0),imshow(reshape(v(:,i),112,92));
```

```
end
   drawnow;
end
[a,i]=min(z)

subplot(122);
b=a/10000
round(b)
if (b<12000)
user_id = ceil(i/10)
imshow(reshape(v(:,i),112,92));
title(' Found!','FontWeight','bold','Fontsize',16,'color','red');
else
user_id = 'not found' ;
title('Not Found!','FontWeight','bold','Fontsize',16,'color','red');

end
```

CHAPTER 4

RESULTS

Following are the results we obtained after testing the above code on various images:

1. The face recognition was successful as the image of the personto be tested was present in the database.

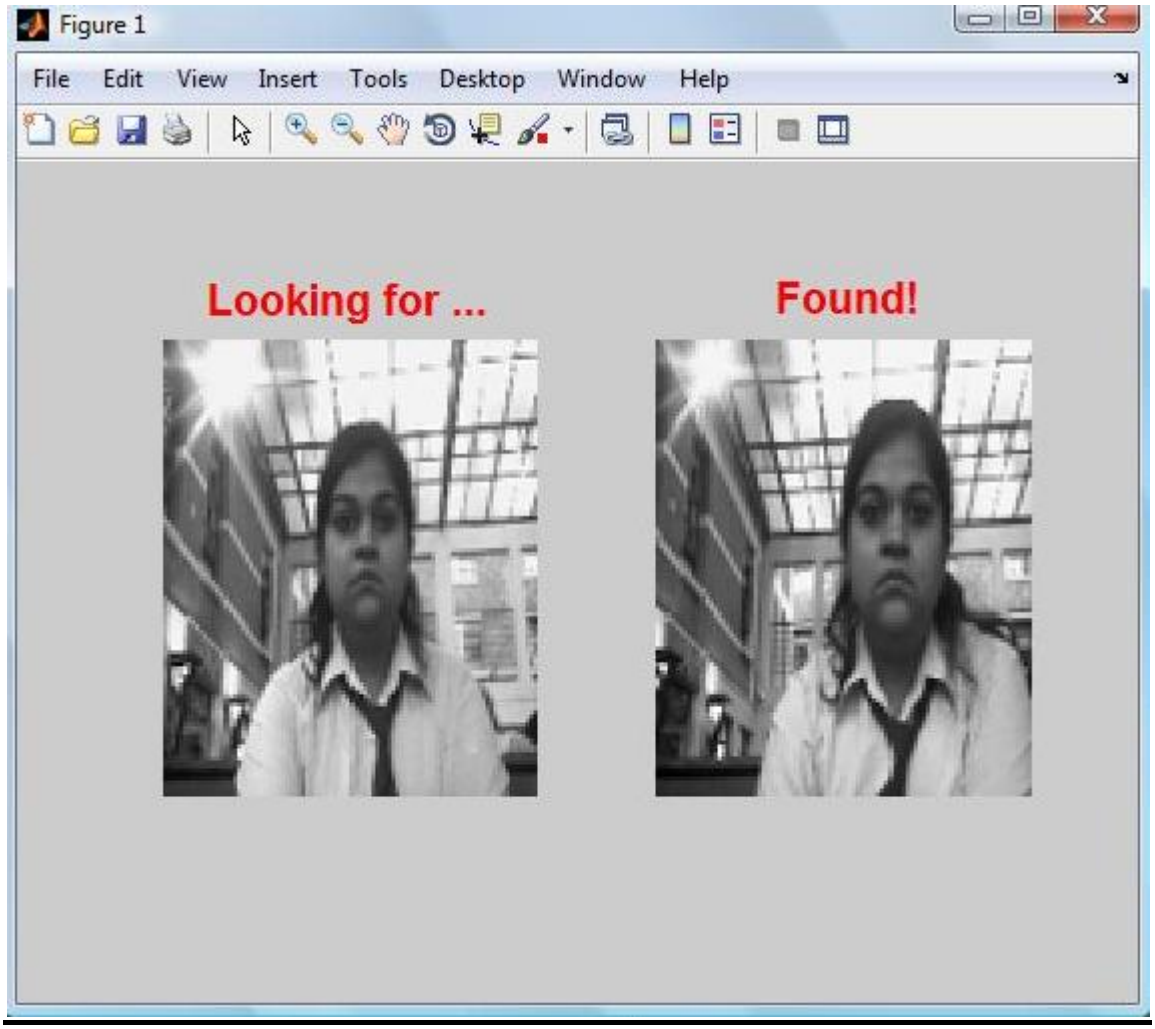


Figure 4.1: Result-1

2. The face recognition was successful as the image of the person to be tested was present in the database

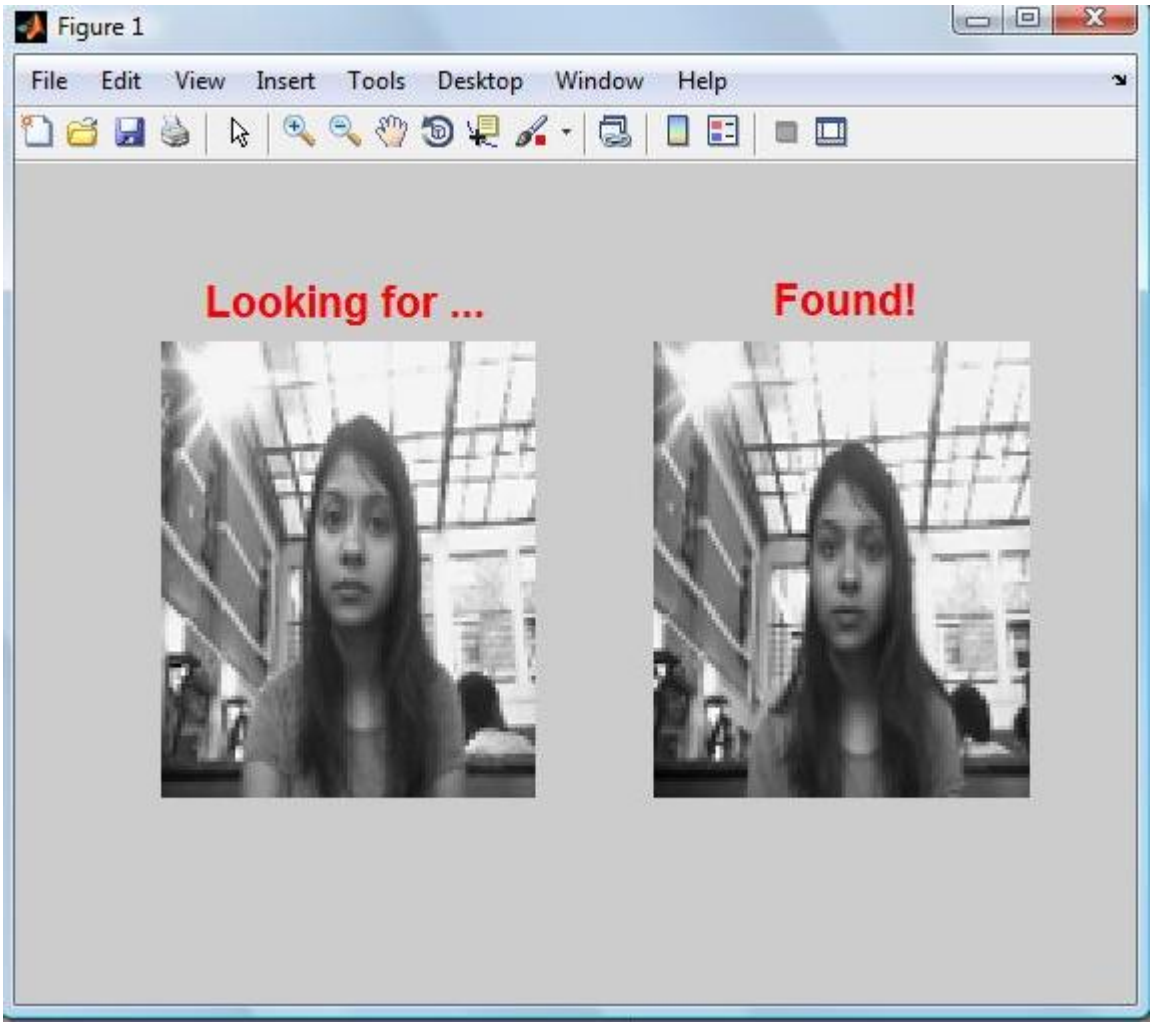


Figure 4.2: Result-2

3. The face recognition was successful even when tested on a different day and in a different environment.

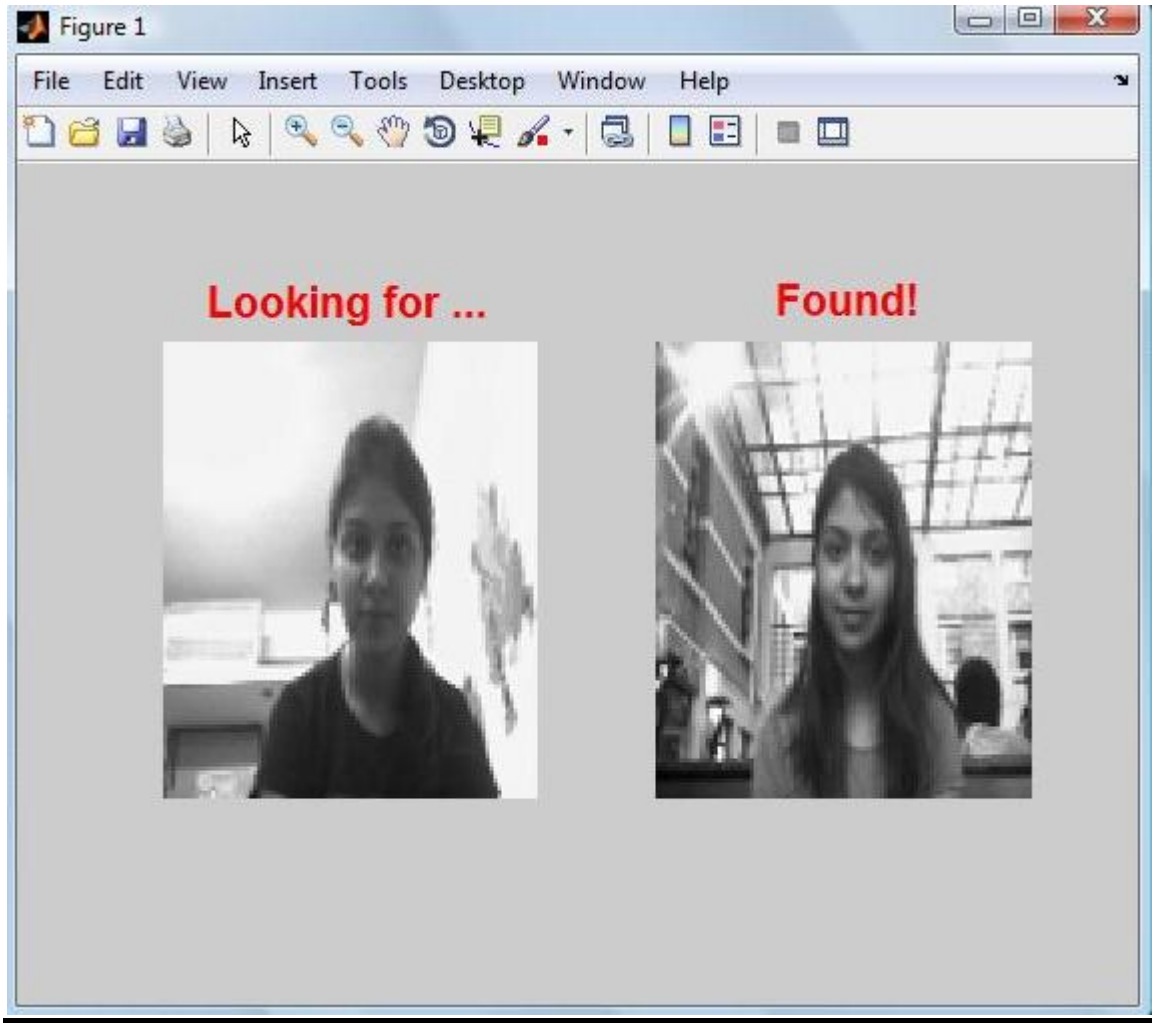


Figure 4.3: Result-3

4. The face recognition was unsuccessful as the image of the person to be tested was not present in the database.

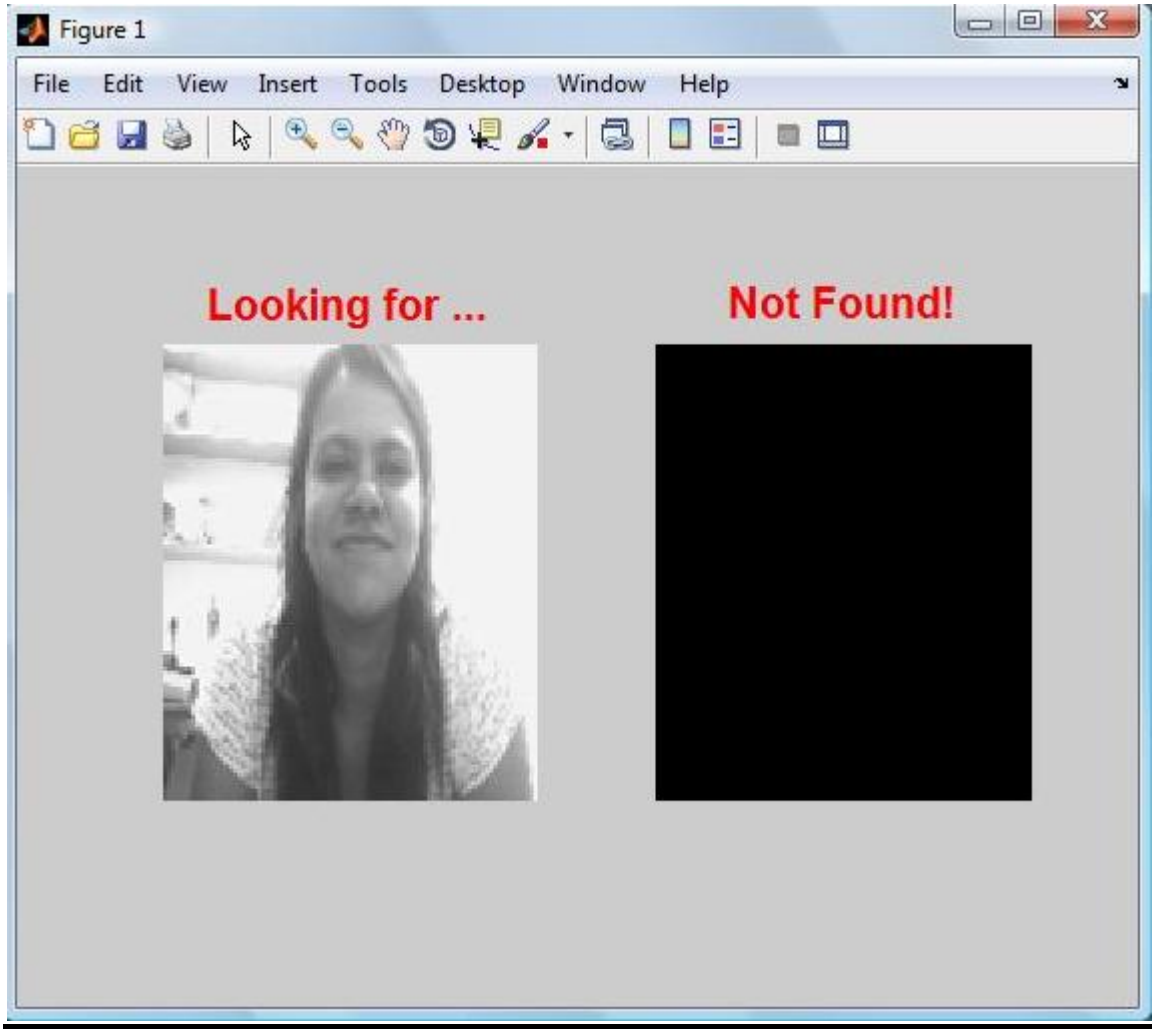


Figure 4.4: Result-4

5. The face recognition was unsuccessful as the image of the person to be tested was not present in the database.

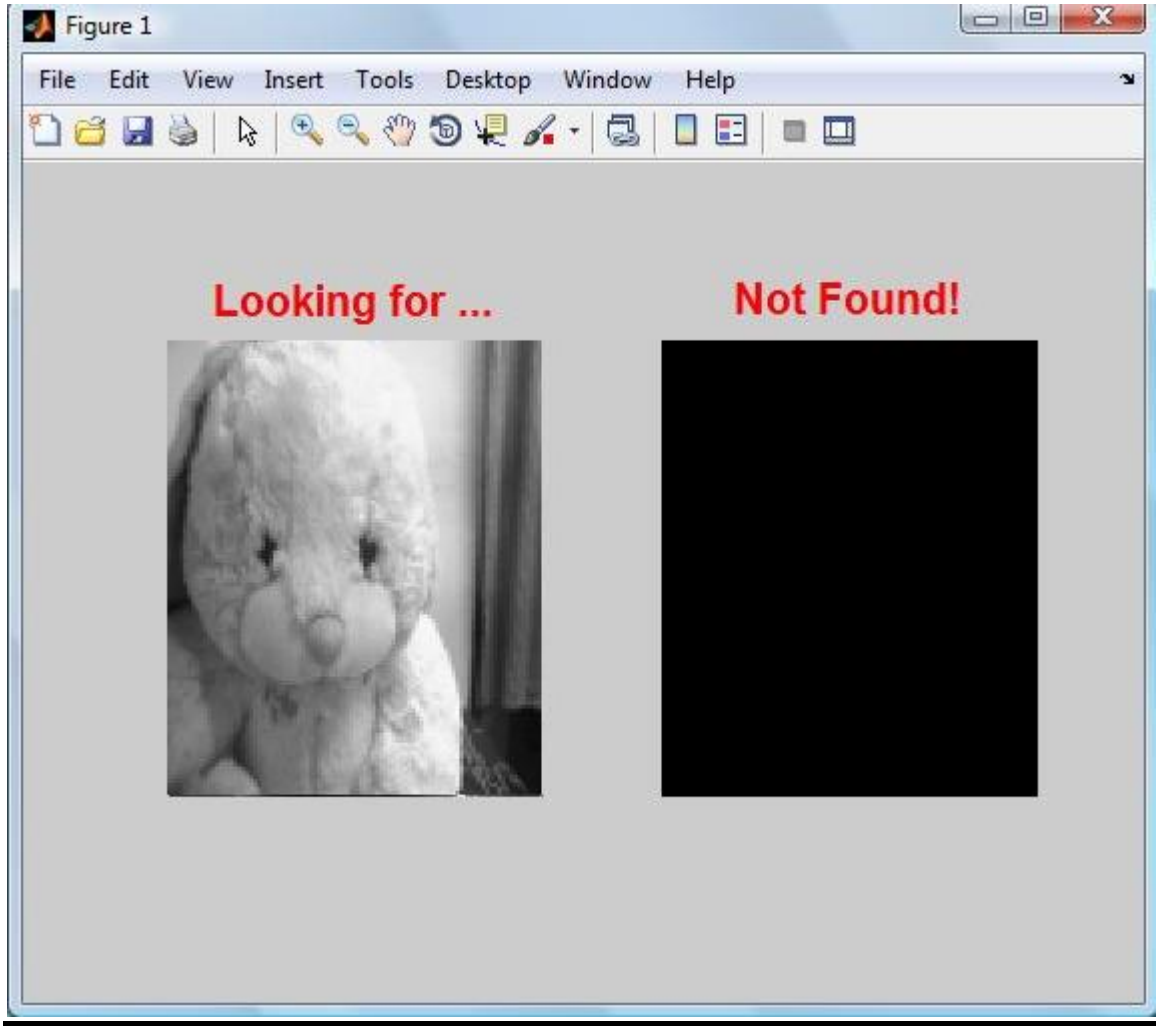


Figure 4.5: Result-5

CHAPTER 5
APPLICATIONS

Face recognition systems are no longer limited to identity verification and surveillance tasks. Growing numbers of applications are starting to use face-recognition as the initial step towards interpreting human actions, intention, and behavior, as a central part of next-generation smart environments. Many of the actions and behaviors humans display can only be interpreted if you also know the person's identity, and the identity of the people around them. Examples are a valued repeat customer entering a store, or behavior monitoring in an eldercare or childcare facility, and command-and-control interfaces in a military or industrial setting. In each of these applications identity information is crucial in order to provide machines with the background knowledge needed to interpret measurements and observations of human actions.

Other potential applications include ATM and check-cashing security. The software is able to quickly verify a customer's face. After a customer consents, the ATM or check-cashing kiosk captures a digital image of him. The "FaceIt" software then generates a faceprint of the photograph to protect customers against identity theft and fraudulent transactions. By using the facial recognition software, there's no need for a picture ID, bankcard or personal identification number (PIN) to verify a customer's identity. This way businesses can prevent fraud from occurring.[16]

Government Uses :

- Law Enforcement. Minimizing victim trauma by narrowing mugshot searches, verifying identify for court records, and comparing school surveillance camera images to known child molesters.
- Security/Counterterrorism. Access control, comparing surveillance images to known terrorists.
- Immigration. Rapid progression through Customs.
- Legislature. Verify identity of Congressmen prior to vote.

- Correctional institutions/prisons. Inmate tracking, employee access.

Commercial Uses:

- Day Care. Verify identity of individuals picking up the children.
- Missing Children/Runaways. Search surveillance images and the internet for missing children and runaways.
- Gaming Industry. Find card counters and thieves.
- Residential Security. Alert homeowners of approaching personnel.
- Internet, E-commerce. Verify identity for Internet purchases.
- Healthcare. Minimize fraud by verifying identity.
- Benefit payments. Minimize fraud by verifying identity.
- Voter verification. Minimize fraud by verifying identity.
- Banking. Minimize fraud by verifying identity.

Evaluating facial recognition systems is very application-specific. Results from an analysis for a specific application are usually not correct for other applications. Evaluating the technology properly is a difficult task for those that have worked in the field for several years, and is even more difficult for those new to the field.

As with many developing technologies, the incredible potential of facial recognition comes with some drawbacks, but manufacturers are striving to enhance the usability and accuracy of the systems.

CHAPTER 6
REFERENCES

[1] R.M. McCabe P.J Phillips and R. Chelleppa, "Biometric image processing and recognition," *in proceedings, European Signal processing Conference*, 1998.

[2] http://www.engineersgarage.com/articles/face-recognition

[3]. Ellis H. Craw, I. and J.R. Lishman, "Automatic extraction of face features.," *Pattern Recognition Letters*, vol. 5, pp. 183–187, February 1987.

[4] http://www.engadget.com/2007/07/16/emotion-recognition-software-knows-you-want-ice-cream/

[5] T. Heseltine, N. Pears, J. Austin, Z. Chen (2003). "Face Recognition: A Comparison of Appearance-Based Approaches". *Proc. VIIth Digital Image Computing: Techniques and Applications*, vol 1. 59-68.

[6] http://en.wikipedia.org/wiki/Facial_recognition_system

[7] http://www.engineersgarage.com/articles/face-recognition

[8] W. Zhao, R. Chellappa, A. Rosenfeld, P. J. Phillips, Face recognition: A literature survey, ACM computing surveys, 2003, pp. 399-458.

[9] http://www.surrey.ac.uk/cvssp/research/facial_analysis/

[10] Ojala, T., Pietikäinen, M. and Harwood, D. (1996), A Comparative Study of Texture Measures with Classification Based on Feature Distributions. Pattern Recognition 19(3):51-59.

[11] http://thehotgadget.com/facebook-use-facial-recognition-technology.html/709/

[12] Amnart Petpon, Sanun Srisuk in 2009 Fifth International Conference on Image and Graphics (2009)

[13] http://www.teachtech.biz/wp-content/uploads/

[14] B. Moghaddam and A. Pentland, Face recognition using view-based and modular eigenspaces //Automatic Systems for the Identification and Inspection of Humans, SPIE Conf. – 1994.- Vol. 2277.-P.1868-1876.

[15] Heusch G., Rodriguez Y. and Marcel S. (2006), eigenvalues as an Image Processing for Face Authentication, Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition.

[16] M. Kirby and L. Sirovich (1990). "Application of the Karhunen-Loeve procedure for the characterization of human faces". *IEEE Transactions on Pattern analysis and Machine Intelligence* **12** (1): 103–108. doi:10.1109/34.41390.