Int. J. Advance. Soft Comput. Appl., Vol. 3, No. 2, July 2011
ISSN 2074-8523; Copyright © ICSRS Publication, 2011
www.i-csrs.org

Implementation of Easy Fingerprint Image Authentication with Traditional Euclidean and Singular Value Decomposition Algorithms

M. James Stephen*, P.V.G.D Prasad Reddy**

* Associate Professor, Dept. of I.T
ANITS, Visakhapatnam
INDIA
jamesstephenm@yahoo.com

** Professor, Dept. of CS & SE
Andhra University, Visakhapatnam
INDIA
prasadreddy.vizag@gmail.com

Abstract

Fingerprints are impression of the friction ridges of the finger. They are used as biometric feature for person identification and verification in the field of biometric identification. In spite of decades of research in fingerprints, reliable finger print recognition is still an open problem. Minutia based fingerprint recognition algorithms have been widely accepted as a standard for single finger recognition applications. This technology has proved to be a reliable form of enrollment and matching in a corporate environment under ideal circumstances. In this paper, an algorithm based on SVD (singular value decomposition) is proposed for feature extraction of a fingerprint and Identification of finger prints is done by using Traditional Euclidean Distance. This paper consists of three main stages (i) Data Acquisition (ii) Feature Extraction and (iii) Authentication / Identification. The image acquisition is done by means of Futronic FS88 fingerprint Scanner. The obtained image is of high quality, 256 gray scale values in every single pixel. The algorithm developed for feature extraction of a fingerprint is based on singular values which are obtained by performing SVD. Identification of finger prints is done by using Euclidean Distance Algorithm. Our experimental results are encouraging. The developed system is light-weighted and simple. The experimental results show that the developed system is efficient and reliable.

Keywords: *Image Processing, Finger Print Identification, Single Value Decomposition algorithm, Euclidean distance.*

1 Introduction

In this highly advancing digital world the level of security is getting breached and also the transaction fraud has increased. Existing security measures rely on knowledge based approaches like passwords, PIN numbers or token based approaches like passports, swipe cards. Such methods are not very secure. These can be easily accessed through number of ways for example by stealing or by sharing etc. Furthermore it is quite impossible to differentiate between authorized user and the person having access to the tokens or passwords. Biometric-based authentication is the perfect solution for this problem. Various classifications of Biometric characteristics are shown in Fig.1.

1.1 Biometrics

Biometrics [1] is the science and technology of measuring and analyzing biological data. It refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Biometric characteristics of human beings can be divided in three main classes,

Physiological are related to the shape of the body. The oldest authentication system that have been used for more than 100 years, are fingerprints. Other examples are face recognition, hand geometry and iris recognition.
Behavioral are related to the behavior of a person. The first characteristic to be used, still widely used today, is the signature. Some more modern approaches are the study of keystroke dynamics and of voice.
Chemical /Biological are related to the chemical analysis of different biological Parameters of a person. This is the latest arena in biometric authentication systems. Some examples are DNA structure analysis, blood glucose, skin spectrography etc.

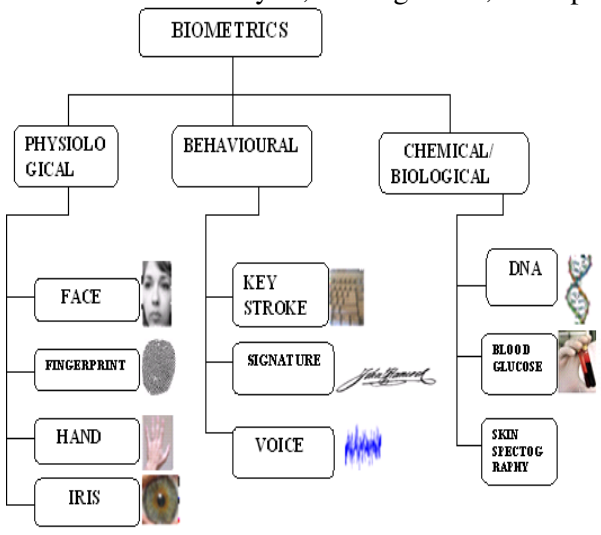

Fig. 1: Classification of Biometric characteristics

1.2 Uses of Biometrics

Biometrics is used in two major ways: Identification and Verification.

Identification is determining who a person is. It involves taking the measured characteristic and trying to find a match in a database containing records of people and that characteristic.

Verification is determining if a person is who they say they are.. It involves taking the measured characteristic and comparing it to the previously recorded data for that person.

1.3 Various Biometric technologies and their comparison

There are various biometric techniques are being used in this post modern age, starting from oldest fingerprint authentication to latest Human Face Emotion Detection [6]. Various existing biometric technologies include Fingerprint, Face, Hand geometry, Key strokes, Hand veins, Iris, Retinal scan, signature, Voice, Facial thermograph, Odor, DNA, Gait, Ear canal and their comparison is given as follow in terms of following parameters [2].

Uniqueness: is how well the biometric separates individually from another.
Permanence: measures how well a biometric resists aging.
Collectability: ease of acquisition for measurement.
Performance: accuracy, speed, and robustness of technology used.
Acceptability: degree of approval of a technology.
Circumvention: ease of use of a substitute.

1.4 Advantages of biometric authentication

There are a number of advantages to this technology:

Biometric identification can provide extremely accurate, secured access to information.
Fingerprints, retinal and iris scans produce absolutely unique data sets when done properly. Current methods like password verification have many problems (people write them down, they forget them, they make up easy-to-hack passwords) Automated biometric identification can be done very rapidly and uniformly Individuals identity can be verified without resort to documents that may be stolen, lost or altered.

1.5 Fingerprints as Biometric

Fingerprint method of identification is the oldest and widely used method of authentication in biometrics authentication. The trait of friction ridge skin means that no two finger prints are ever exactly alike (never identical in every detail), even two impressions recorded immediately after each other, this is the main basis for usage of fingerprints in biometric authentication.

Fingerprints have several advantages over other biometrics, they are as follows:

1.5.1 High universality

A large majority of the human population has legible fingerprints and can therefore be easily authenticated. This exceeds the extent of the population who posses passports, ID cards or any other form of tokens.

1.5.2 High distinctiveness

Fingerprints represent a stronger authentication mechanism than DNA .Even identical twins who share the same DNA have been shown to have different fingerprints, Furthermore, there has been no evidence of identical fingerprints in more than a century of forensic practice.

1.5.3 High permanence

The ridge patterns on the surface of the finger are formed in the womb and remain invariant until death except in the case of severe burns or deep physical injuries.

1.5.4 Easy collectability

The process of collecting fingerprints has become very easy with the advent of online sensors. These sensors are capable of capturing high resolution images of the finger surface within a matter of seconds. This process requires minimal or no user training and can be collected easily from co-operative or non co-operative users. In contrast, other accurate modalities like iris recognition require very co-operative users and have considerable knowledge in using the identification system.

1.5.5 High performance

Fingerprints remain one of the most accurate biometric modalities available to date with jointly optimal FAR (false accept rate) and FRR (false reject rate). In fact its accuracy, speed and robustness exceeded that of face recognition, one of the most popular biometric authentications.

1.5.6 Wide acceptability

While a minority of the user population is reluctant to give their fingerprints due to the association with criminal and forensic fingerprint databases, it is by far the most widely used modality for biometric authentication.

In this paper, we study the common procedure of finger print identification system and then focus on enrollment of finger prints into database. We first analyze the feature extraction of finger prints using Singular Value Decomposition (SVD) algorithm. We then compare the finger print test image and finger print images in the database using Euclidean Distance algorithm and display the result.

The rest of this paper is organized as follows. In Section 2, we give the approaches of finger print identification. In Section 3, we give the stages of finger print authentication. In section 4 we provide the design criteria for finger print recognition. We then analyze the implementation of finger print identification in Section 5. Section 6 describes our experimental results and discussions. Section 7 concludes this paper.

2 Approaches of Finger print Identification

The work carried out in the area of fingerprints identification so far is focused on minutiae extraction [3]. The major Minutiae features of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint.

Before feature extraction process certain pre processing techniques are implemented in order to enhance the image. They are binarization, thinning and segmentation. In binarization technique the obtained gray scale image from sensor is converted into black and white image. In thinning process the image is finely thinned by removing extra pixels. In segmentation process the whole image is divided into small segments so that feature extraction from each segment rather extracting from whole image will be easier. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. The extracted minutiae points are stored in a template in a database and are used for matching with test image features in authentication process.

Like any other approach the minutiae based feature extraction also suffers some limitations. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality as such type of fingerprint images will have very few minutiae. Also this method does not take into account the global pattern of ridges

and furrows. Fingerprint matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns. Local ridge structures cannot be completely characterized by minutiae. It also requires the accurate location of core point and Feature extraction is time consuming process as it involves checking of each and every segment of the fingerprint image. Therefore, SVD based approach is proposed in this Fingerprint Identification System. This approach is mainly used to extract the principal components of the fingerprint. It helps in the simplified representation of the fingerprint which helps to overcome the space and time constraints.

3 Stages of Fingerprint Authentication

Fingerprint identification is an automatic pattern recognition system with three fundamental stages:

1. Data acquisition
2. Feature extraction
3. Matching

The general system architecture of Fingerprint Authentication is depicted in Fig.2

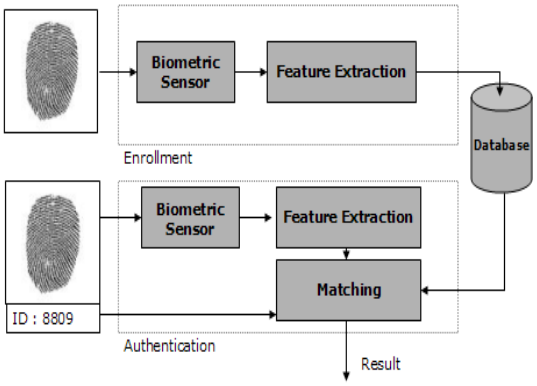

Fig.2: General architecture of Biometric authentication

3.1 Data acquisition:

This is the stage in which data (fingerprint) is acquired through a User interface. The obtained image is stored in database. The proposed system uses *Futronic FS88* fingerprint scanner as user interface.

3.2 Feature extraction:

In this task the features of finger prints are extracted and stored along with its details in the system database. When the fingerprint images are fed to feature extraction module, a feature extraction algorithm is first applied to the image and its features are extracted .The proposed system consists of *SVD* (Singular Value Decomposition) based feature extraction.

3.3 Matching:

The main task of this module is to authenticate identity of a person who intends to access the system. This is the decision making the stage in the architecture. The person to be authenticated indicates his/her identity and places his finger on fingerprint user interface device. A fingerprint image is captured and is fed to a matching module. It extracts the features of the new image and matches with the person's pattern templates stored in the system database. The proposed system consists of Euclidean distance based matching. It involves computation of Euclidean distance between two corresponding SVD points the fingerprint images and comparing it with the threshold.

4 Design Criteria for Finger print Recognition

Finding subsystems during system design is similar to finding objects during analysis. The initial subsystem decomposition should be derived from the functional requirements. The proposed fingerprint authentication system is represented as flowchart in Fig.3
In this paper, there are three subsystems. They are

- Image acquisition
- Feature extraction
- Matching

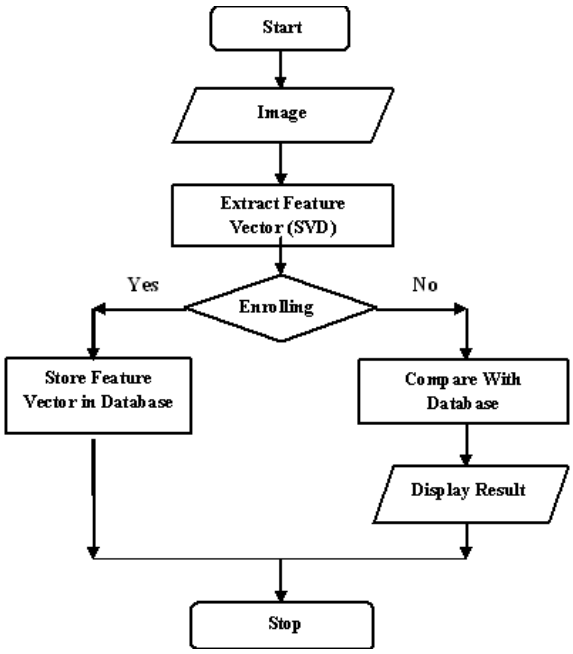

Fig 3: Flow chart of the Fingerprint identification system

4.1 Image acquisition

Fingerprint image acquisition is considered as the most critical step of an automated fingerprint authentication system, as it determines the final fingerprint image quality, which has drastic effects on the overall system performance. On the market there are different types of fingerprint readers, but the basic idea behind each capture approach is the measure in some way the physical difference between ridges and valleys. The procedure to capture a fingerprint using a sensor consists in touching with the finger onto a sensing area, which according to the used physical principle (capacitive, optical, thermal, etc.) captures the difference between valleys and ridges. When a finger touches onto a surface, the elastic skin deforms. The quantity and direction of the pressure applied by the user, the skin conditions and the projection of an irregular 3D object (the finger) onto a 2D flat plane introduce distortions, noise and inconsistencies on the captured fingerprint image. The representation of the same fingerprint changes every time the finger is placed on the sensor platen, so 8 samples per individual are considered and stored as a template in database.

The proposed system uses Futronic FS88 is an optical USB 2.0 fingerprint scanner. The scanner was certified by FBI to be compliant with PIV-071006 Image Quality Specification for Singer Finger Reader. Also FS88 is listed in the

US General Services Administration (GSA) FIPS 201 Evaluation Program Approved Product List.

Technically FS88 scanner is an enhanced version of Futronic FS80 with CMOS image sensor technology and precise optical system. Infra-red LEDs are used to illuminate a finger during scanning. The scanner is able to adapt to fingerprint image quality (wet, dry or blurred fingers) by adjusting illumination intensity. Sensors window is able to resist scratches and other stress.

4.2 Feature extraction

Singular Value Decomposition:

Singular Value Decomposition (SVD) is said to be a significant topic in linear algebra [4]. SVD has many practical and theoretical values. One special feature of SVD is that it can be performed on any real (m,n) matrix. It factors matrix A into three matrices U, S, V, such that, $A = USV^T$ Where U and V are orthogonal matrices and S is a diagonal matrix

The purpose of (SVD) is to factor matrix A into USV ^{T}. The matrix U contains the left singular vectors, the matrix V contains the right singular vectors, and the diagonal matrix S contains the singular values. Where the singular values are arranged on the main diagonal in such an order, it is shown below in equation (1)

$$\sigma_1 \geq \sigma_2 \geq \cdots\cdots \geq \sigma_r > \sigma_{r+1} = \cdots\cdots = \sigma_p = 0, \quad (1)$$

where r is the rank of matrix A, and where (p) is the smaller of the dimensions m or n.

Arbitrary Example:

We begin the process of Singular Value Decomposition by selecting the matrix A which has m rows and n columns. Now, we need to factor A into three matrices U, S, V ^{T} .First we will find V. If we multiply both sides of the equation A = USV ^{T} by A^T we get $A^TA = (USV^T)^T (USV^T) = V S^T U^T USV^T$

Since $U^TU = I$ this gives,

$$A^TA = V S^2 V^T$$

Now we need to diagonalize A^{T}A. This is very similar to the diagonalization of matrix A into A = QQ^T. Except our symmetric matrix is not A, it is A^{T}A. To find V and S we need to find the Eigen values and Eigen vectors of A^{T}A. The Eigen values are the square of the elements of S (the singular values), and the eigenvectors are the columns of V (the right singular vectors). Eliminating V from the equation is very similar to eliminating U. Instead of multiplying on the left by A^T ,we will multiply on the right by A^T. This gives:

$$AA^T = (USV^T)(USV^T)^T = USV^T V S^T U^T .$$

Since $V^T V = I$, this gives

$$AA^T = US^2U^T$$

Again we will find the eigenvectors, but this time for AA^T. These are the columns of U (the left singular vectors). This can be seen in equation (2).

Since A is m × n, S is m × n and A^TA Produces an n × n matrix, and AA^T produces an m × m matrix,

$$A = \begin{pmatrix} u_1 & \cdots & u_r & \cdots & u_m \end{pmatrix} \begin{pmatrix} \sigma_1 & & & & \\ & \ddots & & & \\ & & \sigma_r & & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix} \begin{pmatrix} v_1^T \\ \vdots \\ v_r^T \\ \vdots \\ v_n^T \end{pmatrix} \tag{2}$$

Where U is m × m, S is m × n, V is n × n.

4.3 Matching

Authentication is verified by matching the images in the database with test image**.** The matching algorithm followed in our approach is Euclidean distance based matching.

Euclidean distance:

Euclidean distance is the measure of distance between any two points represented in a two dimensional axis. If the feature vector (SVD) of the test image was calculated as it is shown in equation (3),

$$test\_fv = \{x_1, x_2, x_3, \ldots\ldots\ldots\ldots\ldots\ldots, x_n\} \tag{3}$$

and the feature vector(SVD) of corresponding fingerprint which is stored in the database was retrieved and it is shown in equation (4),

$$db\_fv = \{y_1, y_2, y_3, \ldots\ldots\ldots\ldots\ldots\ldots, y_n\}. \tag{4}$$

Then the Euclidean distance between the two feature vectors is calculated as shown in equation (5)

$$ed = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \ldots\ldots\ldots\ldots + (x_n - y_n)^2}. \quad (5)$$

5 Implementation of Finger print identification

The obtained image from finger print scanner is of high quality, 256 gray scale values in every single pixel. The algorithm developed for feature extraction of a fingerprint is based on singular values which are obtained by performing Singular Value Decomposition (SVD) algorithm. The implementation algorithms are placed in the Appendices.

The test image is taken from the finger print scanner and its feature vectors are extracted. The Euclidean Distance [5] is calculated between the feature vectors of test image and the feature vectors of images present in the database using Euclidean Distance Algorithm. If the distance obtained is less than the Threshold value, status bar displays that the test image is the authenticated match of the user's finger print.

The algorithmic Pseudo code for Enrollment, SVD Algorithm, Verification, Edist algorithm is placed in the Appendices.

6 Experimental Results and Discussions

In order to find out the efficiency of an authentication system it is necessary to find out its measure of likelihood i.e., incorrectly accepting or rejecting an access attempt by an unauthorized or authorized user. False Rejection and False Acceptance are the two measures used to estimate the correctness of the system.

6.1 False Rejection

False Rejection is the instance of a security system failing to verify or identify an authorized person. Also referred to as a *type I error*, a false rejection does not necessarily indicate a flaw in the biometric system; for example, in a fingerprint-based system, an incorrectly aligned finger on the scanner or dirt on the scanner can result in the scanner misreading the fingerprint, causing a false rejection of the authorized user. Table1 shows the analysis for False Rejection. A Total of 680 samples were taken at each time.

Table 1: Analysis for False Rejection

TOTAL SAMPLES	THRESHOLD	FALSE REJECTION	FALSE REJECTION RATE
680	1000	6	0.88
680	1500	2	0.29
680	2000	2	0.29
680	2500	2	0.29

False Rejection Rate:

The false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

6.2 False Acceptance

False Acceptance is the instance of a security system incorrectly verifying or identifying an unauthorized person. It also referred to as a *type II error.* False acceptance typically is considered the most serious of biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out. Table 2 shows the analysis for False Acceptance with a total of 680 samples was taken at each time.

Table 2: Analysis for False Acceptance

TOTAL SAMPLES	THRESHOLD	NO. OF FAULTS	EFFICIENCY (%)
680	1000	12	98.23
680	1500	19	97.20
680	2000	38	94.41
680	2500	76	88.82

False Acceptance Rate

The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an

unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

Table 3: Analysis for False Acceptance Rate

TOTAL SAMPLES	THRESHOLD	FALSE ACCEPTANCE	FALSE ACCEPTANCE RATE
680	1000	6	0.88
680	1500	17	2.50
680	2000	36	5.29
680	2500	74	10.88

Fig. 4 depicts the False Acceptance and False Rejection of the proposed study.

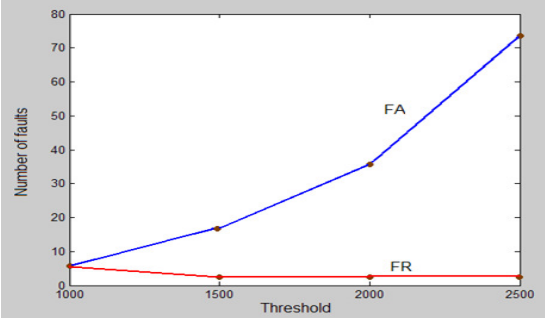

Fig. 4: FA and FR of the proposed study

FR - False Rejection
FA - False Acceptance
Total no. of samples in the database = 680
No. of samples per individual = 8

Efficiency:

The Efficiency of the Finger Print Identification is decided by the Threshold value. Analysis for efficiency is shown in Table 4 and Fig. 5. Again 680 samples were used in this experiment.

Table 4: Analysis of Efficiency

TOTAL SAMPLES	THRESHOLD	FALSE ACCEPTANCE	FALSE ACCEPTANCE RATE
680	1000	6	0.88
680	1500	17	2.50
680	2000	36	5.29
680	2500	74	10.88

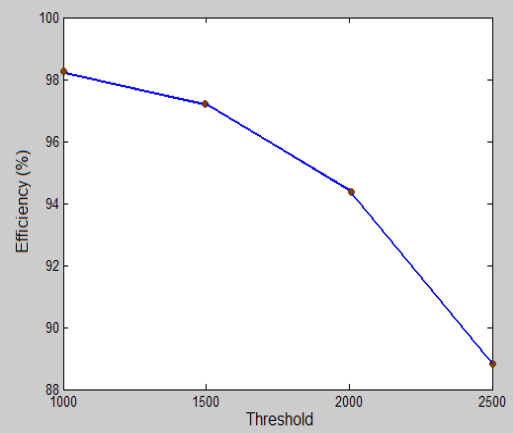

Fig 5: Efficiency of the Finger Print Identification based on the Threshold value

7 Conclusion

The basic principle of SVD is very simple. An image might have many features or characteristics. But it might have (in most cases does) depend upon only some of the features. Also there are space and time constraints in storing all of the features and this property is very useful here. So in order to capture properties of the image with a view to storing them or for further modification one needs only to identify these features and store them. SVD is such a technique. It identifies the main features of the image. It can be done so by performing certain mathematical computations. It allows substantial reduction in the amount of storage required, making large images more manageable and easier to work with. SVD based feature extraction takes less time compared to minutiae based extraction. So SVD is a convenient and powerful technique which can be effectively used for our purposes.

This procedure obtained a False Rejection rate of 0.29% and a False Acceptance rate of 2.5% where as in the filter based algorithm, a False Rejection rate of 14% and a False Acceptance rate of 1% is obtained.

The purpose of this study is to build fingerprint Identification system. This establishes person's identity by searching through a database of available fingerprints associated with known identities. This is the basic functionality of the system. So it is to be understood that the database is an integral part of the software. Hence, the scope of the software can be constrained only due to the size of the database.

References

[1] Biometrics Consortium, http://www.biometrics.org/, 2001-04-15

[2] Jain, A. K. (28-30 April 2004), "Biometric recognition: how do I know who you are?", 12th *IEEE Proceeding on Signal Processing and Communications Applications Conference, 2004,* pp.3 – 5.

[3] U. Halici, L. C. Jain, and A. Erol. An introduction to fingerprint recognition.In, L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, and S. Tsutsui, editors, *Intelligent Biometric Techniques in Fingerprint and Face Recognition,* pp. 3–34, CRC Press, Florida, (1999).

.

[4] Gentle, J. E. "Singular Value Factorization." §3.2.7 in *Numerical Linear Algebra for Applications in Statistics.* Berlin: Springer-Verlag, (1998), pp. 102-103.

[5] Gray, A. "The Intuitive Idea of Distance on a Surface." 15.1 in *Modern Differential Geometry of Curves and Surfaces with Mathematica, 2nd ed.* Boca Raton, FL: CRC Press, pp. 341-345, (1997).

[6] Renu Nagpal, Pooja Nagpal, Sumeet Kaur "Hybrid Technique for Human Face Emotion Detection" *International Journal on Advances in Soft Computing and Its Applications (IJASCA),* Vol.1, No.6, (2010), pp. 87-90.

Appendix

A) Algorithm for Enrollment:

```
en_ret=load('s.mat');
%% Read the file log.txt
[tag image index name]=textread('log.txt','%d %s %d %s');
len=numel(tag);
if(len==0)
   set(handles.edit3,'String',['DATABASE IS EMPTY...']);
end
len=len+1
n=50;
%% Retrieve the tag, image name and the image
ta=len
tf=NaN;

img=en_ret.s.gui_imgname;
nam=en_ret.s.gui_name;
display(ta);
display(nam);
display(img);
tflag=0;

 %%% Check for the existence of the tag
if(len~=1)
   for i=1:(len-1)
       if(isequalwithequalnans(ta,tf)==1)
          set(handles.edit3,'String',['ENTER DETAILS.....']);
          tflag=1;
       elseif(ta==tag(i))
          set(handles.edit3,'String',['TAG EXISTS ALREADY,TRY AGAIN...']);
          tflag=1;
       end
   end
end
if(tflag==0)
   ind=8;  %%Number of samples per student
   samp=1;
   %%Reading multiple images at a time
   [imag,pt] = uigetfile({'*.bmp';'*.tiff'},'ENROLL IMAGE','MultiSelect','on');
   [dummy,filecount]=size(imag);
   fileflag=1;
```

```
   if(filecount~=ind)
      set(handles.edit3,'String',['SELECT 8 SAMPLES']);
      fileflag=0;
   end
   r1=0;
   abnormalflag=1;
   if(filecount==ind)
      for fi=1:ind
         %% Check for abnormality
         [ab]=abnormal(imag{fi});
         if(ab==1)
            abnormalflag=0;
            [SAMPLE]=sprintf('%s %s',imag{fi},'IS ABNORMAL IMAGE');
            display(SAMPLE);
            r1=1;
         end
      end
   end

   while((samp<=ind)&(fileflag==1)&(abnormalflag==1))
      %% Find the svd of the input images
      op=svd_ip(imag{samp});
      l=size(op);
      for temp=1:l
         k(1,temp)=op(temp);
      end
      %% Write feature vectors to a text file
      dlmwrite('FV.txt',k,'-append');
      [SAMPLE]=sprintf('%d %s %s',samp,imag{samp},'ENROLLED');
      display(SAMPLE);
      samp=samp+1;
   end
   if(fileflag==1 & abnormalflag==1)
      %% Write the user entries to a log file
      write_txt(ta,img,ind,nam);
      set(handles.edit3,'String',['SUCCESSFULLY ENROLLED']);
   end
end
%%% Clear the edit text boxes
set(handles.edit4,'String',['     ']);
set(handles.edit2,'String',['     ']);
```

B) SVD Algorithm:

```
function op=svd_ip(ipimg)
img=imread(ipimg);
k=double(img);
n=50;          %%%%%%%% vector length
[u,s,v]=svd(k,0);
temp=diag(s);
temp=round(temp);
op=temp(1:n);
return;
```

C) Algorithm for Verification:

```
global s;
%%Read the user tag number
s.gui_tag=str2double(get(hObject,'string'));
save s;
test_tag=s.gui_tag;
k=load('fn_img.mat');
fn=k.fn_img;
%%Read the file FV.txt
sdv=dlmread('FV.txt');
%% Read the file log.txt
[tag image index name]=textread('log.txt','%d %s %d %s');
%% Find the number of tags
len=numel(tag);
tflag=0;
tagind=0;
%% Thresold for matching
thres=1500;
%%Feature vector length
n=25;
for i=1:len
   if(test_tag==tag(i))
      tflag=1;
      ind=i;
      break;
   else tagind=tagind+index(i);
   end
end
if(tflag==1)
   set(handles.edit2,'String',['TAG EXISTS...']);
   %% Call the function to find the abnormality
```

```
   [ab]=abnormal(fn);
   if(ab==1)
set(handles.edit2,'String',['ABNORMAL IMAGE,TRY AGAIN...']);
   else
      %%Find the svd if the input image
      d2=svd_ip(fn);
      tagind=tagind+1;
      ii=1;
      for i=tagind:(tagind+index(ind)-1)
         d1=sdv(i,:);
         testd(ii,:)=d1;
         ed(ii)=round(edist(d1,d2));  %%% CALL FUNCTION edist
         mi=min(ed);
         ii=ii+1;
      end
      if(mi<=thres)
         set(handles.edit2,'String',['MATCH FOUND']);
else
         set(handles.edit2,'String',['MATCH NOT FOUND']);
      end
   end
else
   set(handles.edit2,'String',['TAG DOES NOT EXIST...']);
end
set(handles.edit1,'String',['     ']);
```

D) Edist Algorithm:

```
function e_dist=edist(d1,d2)
x=numel(d1);
e_dist=0;
for i=1:x
   e_dist=e_dist+(d1(i) - d2(i))*(d1(i) - d2(i));
end
e_dist=sqrt(e_dist);
% display(e_dist);
End
```