An Application of Face Recognition System using Image Processing and Neural Networks

Rakesh Rath (Ph.D.)*1, Manish Choudhary (M.Tech.)*2, Bhuwan Chandra(Ph.D.)*3

1 Department of Computer Engineering & I.T., Govt. Engineering College, Ajmer, India
2 Department of Computer Engineering & I.T., Govt. Engineering College, Ajmer, India
3 Departments of Computer Engineering & I.T., Research Scholar, Singhai University, Pacheri Bari, Jhunjhunu

Corresponding Author: e-mail: rakeshrathi4@rediffmail.com
Corresponding Author: e-mail: chowdhary_2000@rediffmail.com
Corresponding Author: e-mail: bcd_hald@yahoo.com

Abstract—In recent years face recognition has received substantial attention from both research communities and the market, but still remained very challenging in real applications. A lot of face recognition algorithms, along with their medications, have been developed during the past decades. A number of typical algorithms are presented.

In this paper, we propose to label a Self-Organizing Map (SOM) to measure image similarity. To manage this goal, we feed Facial images associated to the regions of interest into the neural network. At the end of the learning step, each neural unit is tuned to a particular Facial image prototype. Facial recognition is then performed by a probabilistic decision rule. This scheme offers very promising results for face identification dealing with illumination variation and facial poses and expressions. This paper presents a novel Self-Organizing Map (SOM) for face recognition. The SOM method is trained on images from one database. The novelty of this work comes from the integration of a Facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the way is to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

Keywords: Face recognition, self-organizing map, neural network, artificial intelligence, scope.

1. Introduction

It is often useful to have a machine perform pattern recognition. In particular, machines which can read face images are very cost effective. A machine that reads passenger passports can process many more passports than a human being in the same time [1]. This kind of application saves time and money, and eliminates the requirement that a human perform such a repetitive task. This document demonstrates how face recognition can be done with a back propagation artificial neural network.

Recognition System (FRS) can be subdivided into two main parts. The first part is image processing and the second part is recognition techniques. The image processing part consists of Face image acquisition through scanning. Image enhancement, Image clipping, Filtering, Edge detection and Feature extraction. The second part consists of the artificial intelligence which is composed by Genetic Algorithm and

Fig1. Generic representation of a face recognition system

Geometric approach to face recognition

The first historical way to recognize people was based on face geometry. There are a lot of geometric features based on the points. We experimentally selected 37 points. Geometric features may be generated by segments, perimeters and areas of some figures formed by the points. To compare the recognition results we studied the feature set described in detail in [7]. It includes 15 segments between the points and the mean values of 15 symmetrical segment pairs. We tested different subsets of the features looking for the most important features. tested 70 images of 12 persons. Images of two persons were added from our image database. They were done with a huge time difference (from 1 to 30 years). We have selected 28 features. In spite of small rotation, orientation and illumination variances, the algorithm works in a fairly robust manner. Each image was tested as a query and compared with others. Just in one case of 70 tests there were no any image of the person in the query through the 5 nearest ones, i.e. the recognition rate was 98.5%. The approach is robust, but it main problem is automatic point location. Some problems arise if image is of bad quality or several points

Fig2. Some facial points and distances between them are used in face recognition.
Neural Networks for Access Control

Face Recognition is a widespread technology used for Access Control. The task is stated as follows. There is a group of authorized people, which a recognition system must accept. All the other people are unauthorized or ‘aliens’ and should be rejected. We can train a system to recognize the small group of people that is why application of a Multilayer Perceptron (MLP) Neural Network (NN) was studied for this task. Configuration of our MLP was chosen by experiments. It contains three layers. Input for NN is a gray scale image. Number of input units is equal to the number of pixels in the image. Number of hidden units was 30. Number of output units is equal to the number of persons to be recognized. Every output unit is associated with one person. NN is trained to respond “+1” on output unit, corresponding to recognized person and “-1” on other outputs. We called this perfect output. After training highest output of NN indicates recognized person for test image. Most of these experiments were passed on ORL face database. Any input image was previously normalized by angle, size, position and lightning conditions. We also studied other image representations: a set of discrete cosine transform coefficients and a gradient map. Using DCT first coefficients we reduce the sample size and significantly speedup the training process. DCT representations allow us to process JPEG and MPEG compressed images almost without decompression. A gradient map allows to achieve partial invariance to lightning conditions. In our experiments with NNS we studied several subjects. We explored thresholding rules allowing us to accept or reject decisions of NN. We introduced a thresholding rule, which allow improving recognition performance by considering all outputs of NN. We called this ‘sqr’ rule. It calculates the Euclidean distance between perfect and real output for recognized person. When this distance is greater than the threshold we reject this person. Otherwise we accept this person. The best threshold is chosen experimentally.

Challenges in Face Recognition: - Pose, Illumination, Facial expression, Image condition, Face size.

Classification of Face Recognition

Face recognition scenarios can be classified into two types Face verification (or authentication) and Face identification (or recognition).

1) Face verification: It is a one-to-one match that compares a query face image against a template face image whose identity is being claimed. To evaluate the verification performance, the verification rate (the rate, at which legitimate users are granted access) vs. false accepts rate (the rate at which imposters are granted access) is plotted, called ROC curve. A good verification system should balance these two rates based on operational needs.

2) Face identification: It is a one-to-many matching process that compares a query face image against all the template images in a face database to determine the identity of the query face. The identification of the test image is done by locating the image in the database that has the highest similarity with the test image [4]. The identification process is a “closed” test, which means the sensor takes an observation of an individual that is known to be in the database. The test subject’s (normalized) features

2. Problem Formulation

There is a database of N portrait images and a query image. Find k images most similar to the given face image. The number k may be a constant (for example, 20 for a large database), it may be limited by a similarity threshold, or it may be equal to the number of all pictures of the same person in the database.

Input image normalization

Image normalization is the first stage for all face recognition systems. Firstly face area is detected in the image. We used template matching to localize a face. Then the eye (iris) centers should be detected because the distance between them is used as a normalization factor. We located the eyes in facial images of different size using the luminance.

Input Data Limitation

For robust work of the system, images must satisfy the following conditions:

- They are gray-scale or color digital photos.
- The head size in the input image must be bigger than 60x80 pixels; otherwise the fiducially points may be detected with low accuracy.
- Intensity and contrast of the input image allow detecting manually the main anthropometrical points like eye corners, nostrils, lipping contour points, etc.
- The head must be rotated not more than at 15-20 degrees (with respect to a frontal face position). Ideally, the input image is a digitized photo for a document (Passport, driving license, etc.).

3. Neural network

The network will receive the 960 real values as a 960-pixel input image (Image size ~ 32 x 30). It will then be required to identify the face by responding with a 94-element output vector [5]. The 94 elements of the output vector each represent a face. To operate correctly the network should respond with a 1 in the position of the face being presented to the network All other values in the output vector should be 0 [5]. In addition, the network should be able to handle noise. In practice the network will not receive a perfect image of face which represented by vector as input. Specifically, the network should make as few mistakes as possible when classifying images with noise of mean 0 and standard deviation of 0.2 or less.
4. Architecture of Neural Network

The neural network needs 960 inputs and 94 neurons in the output layer to identify the faces. The network is a two-layer log-sigmoid/log-sigmoid network [6], [7], [8]. The log-sigmoid transfer function was picked because its output range (0 to 1) is perfect for learning to output Boolean values (see figure 3) [5].

![Fig3. Architecture of neural network](image)

The hidden layer has 200 neurons [5]. This number was picked by guesswork and experience [5]. If the network has trouble learning, then neurons can be added to this layer [5], [9]. The network is trained to output a 1 in the correct position of the output vector and to fill the rest of the output vector with 0’s. However, noisy input images may result in the network not outputting perfect 1’s and 0’s. After the network has been trained, the output will be passed through the competitive transfer function. This function makes sure that the output corresponding to the face most like the noisy input image takes on a value of 1 and all others have a value of 0. The result of this post-processing is the output that is actually used [9].

5. Training

To create a neural network that can handle noisy input images, it is best to train the network on both ideal and noisy images. To do this, the network will first be trained on ideal images until it has a low sum-squared error. Then the network will be trained on 10 sets of ideal and noisy images. The network is trained on two copies of the noise-free database at the same time as it is trained on noisy images. The two copies of the noise-free database are used to maintain the network’s ability to classify ideal input images. Unfortunately, after the training described above, the network may have learned to classify some difficult noisy images at the expense of properly classifying a noise-free image. Therefore, the network will again be trained on just ideal images. This ensures that the network will respond perfectly when presented with an ideal face. All training is done using back propagation with both adaptive learning rate and momentum.

5.1. Training without noise (network 1 “net”)

The network is initially trained without noise for a maximum of 10,000 epochs or until the network sum-squared error falls below 0.1 (see this figure).

5.2. Training with noise (network 2 “net N”)

To obtain a network not sensitive to noise, we trained with two ideal copies and two noisy copies of the images in database. The noisy images have noise of mean 0.1 (“salt & pepper” noise) and 0.2 (“Poisson” noise) added to them. This forces the neurons of the network to learn how to properly identify noisy faces, while requiring that it can still respond well to ideal images. To train with noise, the maximum number of epochs is reduced to 300 and the error goal is increased to 0.6, reflecting that higher error is expected due to more images, including some with noise, being presented.

5.3. Training without noise again

Once the network has been trained with noise, it makes sense to train it without noise once more to ensure that ideal input images are always classified correctly.

6. System performance

The reliability of the neural network pattern recognition system is measured by testing the network with hundreds of input images with varying quantities of noise. We test the network at various noise levels and then graph the percentage of network errors versus noise. Noise with mean of 0 and standard deviation from 0 to 0.5 are added to input images. At each noise level, 100 presentations of different noisy versions of each face are made and the network’s output is calculated. The output is then passed through the competitive transfer function so that only one of the 94 outputs, representing the faces of the database, has a value of 1. The number of erroneous classifications is then added and percentages are obtained (see figure):
The solid line (black line) on the graph shows the reliability for the network trained with and without noise. The reliability of the same network when it had only been trained without noise is shown with a dashed line. Thus, training the network on noisy input images of face greatly reduced its errors when it had to classify or to recognize noisy images. The network did not make any errors for faces with noise of mean 0.00 or 0.05. When noise of mean 0.10 was added to the images both networks began to make errors. If a higher accuracy is needed the network could be trained for a longer time or retrained with more neurons in its hidden layer. Also, the resolution of the input images of face could be increased to say, a 640 by 480 matrix. Finally, the network could be trained on input images with greater amounts of noise if greater reliability were needed for higher levels of noise.

7. Test

To test the system, a face with noise can be created and presented to the network [5], [10]. (See table 1 for more example of faces with different kind of noise).

Table 1. Recognition results on the face image database (Image size ~ 32 x 30) on a PC with 1.7 GHz CPU, RR: Recognition Rate.

<table>
<thead>
<tr>
<th>Architecture Of Neural Network</th>
<th>Training</th>
<th>Time of Training</th>
<th>Recognition Rate (RR)</th>
<th>Database With Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artificial Neural Network 1</td>
<td>Train</td>
<td>51 min</td>
<td>100 %</td>
<td>Salt &amp; Pepper noise</td>
</tr>
<tr>
<td>“Net”</td>
<td>Test</td>
<td>5 min</td>
<td>100 %</td>
<td>Poison noise</td>
</tr>
<tr>
<td>Artificial Neural Network 2</td>
<td>Train</td>
<td>42 sec</td>
<td>100 %</td>
<td>Speckle noise</td>
</tr>
<tr>
<td>“Net”</td>
<td>Test</td>
<td>6 min</td>
<td>100 %</td>
<td>Gaussian noise</td>
</tr>
</tbody>
</table>

8. Scope in India

1) In order to prevent the frauds of ATM in India, it is recommended to prepare the database of all ATM customers with the banks in India & deployment of high resolution camera and face recognition software at all ATMs. So, whenever user will enter in ATM his photograph will be taken to permit the access after it is being matched with stored photo from the database.

2) Duplicate voter are being reported in India. To prevent this, a database of all voters, of course, of all constituencies, is recommended to be prepared. Then at the time of voting the resolution camera and face recognition equipped of voting site will accept a subject face 100% and generates the recognition for voting if match is found.

3) Passport and visa verification can also be done using face recognition technology as explained above.

4) Driving license verification can also be exercised face recognition technology as mentioned earlier.

5) To identify and verify terrorists at airports, railway stations and malls the face recognition technology will be the best choice in India as compared with other biometric technologies since other technologies cannot be helpful in crowded places.

6) In defense ministry and all other important places the face technology can be deployed for better security.

7) This technology can also be used effectively in various important examinations such as SSC, HSC, Medical, Engineering, MCA, MBA, B- Pharmacy, Nursing courses etc. The examinee can be identified and verified using Face Recognition Technique.

8) In all government and private offices this system can be deployed for identification, verification and attendance.

9) It can also be deployed in police station to identify and verify the criminals.

10) It can also be deployed vaults and lockers in banks for access control verification and identification of authentic users.

11) Present bar code system could be completely replaced with the face recognition technology as it is a better choice for access & security since the barcode could be stolen by anybody else.

9. Conclusion and future Work

Face recognition is both challenging and important recognition technique. Among all the biometric techniques, face recognition approach possesses one great advantage, which is its user-friendliness (or non-intrusiveness). In this paper, we have given an introductory survey for the face recognition technology. We have covered issues such as the generic framework for face recognition, factors that may affect the performance of the recognizer, and several state-of-the-art face recognition algorithms. We hope this paper can provide the readers a better understanding about face recognition, and we encourage the readers who are interested in this topic to go to the references for more detailed study.
Face recognition technologies have been associated generally with very costly top secure applications. Today the core technologies have evolved and the cost of equipments is going down dramatically due to the integration and the increasing processing power. Certain applications of face recognition technology are now cost effective, reliable and highly accurate. As a result there are no technological or financial barriers for stepping from the pilot project to widespread deployment. Though there are some weaknesses of facial recognition system, there is a tremendous scope in India. This system can be effectively used in ATM’s, identifying duplicate voters, passport and visa verification, driving license verification, in defense, competitive and other exams, in governments and private sectors.

Government and NGOs should concentrate and promote applications of facial recognition system in India in various fields by giving economical support and appreciation.

There are a number of directions for future work. The main limitation of the current system is that it only detects upright faces looking at the camera. Separate versions of the system could be trained for each head orientation, and the results could be combined using arbitration methods similar to those presented here. Preliminary work in this area indicates that detecting pro files views of faces is more difficult than detecting frontal views, because they have fewer stable features and because the input window will contain more background pixels.

10. References