STM JOURNALS

Journal of Artificial Intelligence Research & Advances
ISSN: 2395-6720(online)
Volume 2, Issue 3
www.stmjournals.com

Detection System in Human Face using Biometrics

P Priya*
Department of MCA, AVS College of Arts and Science, Salem, Tamilnadu, India

Abstract

A person is identified with face. Face recognition is one of biometric methods, to identify given face image using main features of face. Biometrics is a growing technology, which has been widely used in forensics, secured access and prison authentication. A biometric system is fundamentally a pattern recognition system that recognizes a person by determining the secured by using his different biological features i.e. fingerprint, retina-scan, iris scan, hand geometry, and face recognition are highly qualified physiological biometrics; and behavioral characteristic are voice recognition, keystroke-scan, and signature-scan. In this paper we discussed about face recognition system.

Keywords*: Face recognition, biometrics, biometric recognition*

****Author for Correspondence*** E-mail: priyaplrj@gmail.com

INTRODUCTION

Face detection is an essential tool for face recognition system. It is a recognition process that analyzes facial characteristics of a person. Humans can easily recognize faces, spoken words, handwritten or printed digits, images and many other things in everyday life. If there are a limited number of categories or classes then recognition performance may be improved; however, the same might not be very efficient if several categories are present. Face recognition is a natural and straightforward biometric method used by us to identify one another [1].

The recent interest in face recognition can be attributed to the use of latest techniques in security and surveillances and many other commercial interests. People look for more secure methods to protect their valuable information. Password authentication, card key authentication, and biometric authentication are the most commonly used authentication types. It has numerous applications such as surveillance, security control systems, content based image retrieval, video conferencing, and intelligent human computer interfaces. Most of the current face recognition systems presume that faces are readily available for processing. However, one cannot get typical images with just faces. The corollary is that a system that will segment faces into cluttered images is needed [2–4]. With such a portable system, one can ask the user to pose for the face identification task. In addition to creating a more cooperative target, one can also interact with the system in order to improve and monitor face detection. With a portable system, detection seems easier.

OBLIGE FOR FACE DETECTION

A facial recognition system is computer application which can automatically identify or verify a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features of the image and a facial database. It is typically used in security systems and other biometrics such as fingerprint or eye iris recognition systems.

There are number of potential uses for facial recognition that are currently being developed. For example, the technology could be used as a security measure at ATM's, instead of using a bank card or personal identification number; the ATM would capture an image of your face, and compare it to your photo in the bank database to confirm your identity. Security systems use biometrics for two basic purposes: to verify or to identify users [5, 6].

Identification tends to be the more difficult of the two uses because a system must search a database of enrolled users to find a match (a one-to-many search). The biometric that a

security system employs depends in part on what the system is protecting and what it is trying to protect against. The same concept could also be applied to computers, by using a webcam to capture a digital image of yourself and your face could replace your password as a means to log-in in the system. A face recognition system has a lot of commercial, military, security and research applications. Some of them are:

- Detection of a criminal at public place.
- Can be used in different areas of science for comparing an entity with a group of entities.
- Pattern recognition.
- Checking for criminal records.
- Enhancement of security by using surveillance cameras in conjunction with face recognition system.
- Knowing in advance, if some VIP is entering the hotel.

BIOMETRIC TECHNOLOGY

Biometric technology is one area that no segment of the IT industry can afford to ignore. Biometrics provides security benefits across the spectrum, from IT vendors to end users, and from security system developers to security system users.

All these industry sectors must evaluate the costs and benefits of implementing such security measures. Different technologies may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters. Biometric technology has been around for decades but has mainly been for highly secretive environments with extreme security measures. The technologies behind biometrics are still emerging. We can classify the biometric techniques into two classes:

- **Physiological based Techniques**

They include facial analysis, fingerprint, hand geometry, retinal analysis, DNA and measure the physiological characteristics of a person.

- **Behavior based Techniques**

They include signature, key stroke, voice, smell, sweat pores analysis and measure behavioral characteristics.

Biometric recognition systems based on the above methods can work in two modes: identification mode, where the system identifies a person searching a large data base of enrolled for a match; and authentication mode where the system verifies a person's claimed identity from his earlier enrolled pattern.

Vendors often use two different methods to rate biometric accuracy: false-acceptance rate or false-rejection rate. Both methods focus on the system's ability to allow limited entry to authorized users. However, these measures can vary significantly, depending on how you adjust the sensitivity of the mechanism that matches the biometric. For example, you can require a tighter match between the measurements of hand geometry and the user's template (increase the sensitivity). This will probably decrease the false-acceptance rate, but at the same time can increase the false-rejection rate. So be careful to understand how vendors arrive at quoted values of FAR and FRR. Because FAR and FRR are interdependent, it is more meaningful to plot them against each other. Each point on the plot represents a hypothetical system's performance at various sensitivity setting.

A MIXTURE OF BIOMENTRIC RECOGNITION SYSTEM

Many biometric systems are available in various applications. Biometric means "life measurement". Each human acquires some sole physiological characters to identify a person. There is no biometric which is optimal; depending upon the application they were used. A brief introduction of commonly used biometrics is given below:

Fingerprint Recognition

Fingerprint biometric is widely used in various fields for security. Fingerprint identification are used for past many years by matching. A fingerprint contains patterns of valley and ridges on the surface of finger tips. Even for twins the fingerprint won't be same. It is probable that two individuals having same fingerprint are less than one in billion [7, 8].

The cost of this biometric is low and they were embedded in laptops also. The accuracy of current biometric system is adequate for

verification. Only one problem in current biometric that it requires large amount of computational resource, when using in identification mode. Finally the fingerprint biometric is not suitable for some factors like aging, environmental or occupation reason (e.g.: manual workers who use hands frequently for their work). The main advantages of fingerprint biometrics are: easy to use, economical, very high accuracy and small size for template. The disadvantages are: change quickly for children, compose mistake with dryness or dirt in fingers and a cut or scar on finger.

Iris Recognition

Iris recognition is an automated method of biometric identification that uses mathematical path recognition technique. The visual texture of iris is formed during fetal development and becomes stable in first two years itself. Iris recognition is also widely used, it is feasible in large scale. Each iris is different for twins like finger print. It is extremely difficult to change iris pattern and it's easy to detect the artificial iris. For iris scan, a specialized camera is required. The complete process will take few seconds only.

The main advantages of iris recognition are: very high accuracy, and verification times takes less than five seconds. The disadvantage of this recognition are: cost is high, too much movement of head and use of color contact lens.

DNA Recognition

Deoxyribo nucleic acid (DNA) is the one dimensional unique pattern for one's individuality but in case of identical twins have identical DNA patterns. This technology is mostly used in forensics application for person recognition. DNA recognition has three main issues to limit the utilization of this biometrics for other application:

(i) Contamination process and sensitivity module: Easy to take a portion of DNA.
(ii) Automatic recognition issues in real time: The current technology for DNA pattern matching requires cumbersome chemical method involving an expert's skill.
(iii) Privacy issues: With the DNA pattern of a person certain diseases can be gained.

Hand and Finger Geometry

Hand geometry recognition system is based on measurements taken from the human hand, which includes shape, size and length and widths of fingers. Commercial hand geometry based verification systems were used in various places around the world. This technique is very simple, easy to use and also inexpensive. Environmental factors such as dry weather won't affect the verification accuracy of hand geometry based system. Hand geometry information may not be invariant during growth period of children.

Palm Print Recognition

Palm print recognition is more or like finger print recognition, both contain pattern of ridges and valleys. The size of the palm is larger comparing to the finger, as a result palm print scanner needs to capture larger area and also they are more expensive. Human palm contains some additional distinctive features such as principal lines and wrinkles that can be captured with low resolution scanner, which would be cheap. So with the help of high resolutions scanners all features of palm such as hand geometry, ridges and valleys features, principal lines and wrinkles can be extracted to build highly accurate biometric system.

Signature Recognition

Signature verification method is used in various fields like government, legal and commercial transactions. Signature is a behavioral biometric that can change over a period of time. Signature of some people varies substantially: even successive an impression of their signature looks different. Further professional forgers may able to reproduce signature that freaks the system.

Voice Recognition

Voice is the combination of physiological and behavioral biometrics. The physiological characteristic of human voice may be unique but the behavioral characteristic of human may change over a period of time due to illness, age, emotional state, etc. Voice is also not very distinctive and may not be suitable for large scale identifications. Text dependent voice recognition system is based on the pitch of a predetermined phrase. It is more difficult to design a text independent system than text

dependent systems but offers high security against fraud.

FACE DETECTION SYSTEM

In order to recognize a person, one commonly looks at faces, which differentiate one person from another. Humans often use faces to recognize individuals and advancements in computing capability over the past few decades now enable similar recognitions automatically. Early face recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes.

Major Advancements and Initiatives in the Past Ten to Fifteen Years

Eyes in particular seem to tell a story not only about who somebody is, but also about how that person feels, where his/her attention is directed, etc. Face recognition records the spatial geometry of unique features of the face. Main focus is on key features of the face. Face recognition technique is used to identify terrorists, criminals, and other types of persons for law enforcement purposes. This is a non intrusive, cheap technology. In 2D; recognition is affected by change in lighting, the person's hair, age, and if the people wear glasses, low resolution images.

It requires camera as equipment for user identification; thus, it is doubtful to become popular until most PCs include cameras as standard equipment. United States used same technologies to prevent people from obtaining fake identification cards and driver's licenses. Face recognition has always been a very challenging task for the researches. On the one hand, its applications may be very useful for personal verification and recognition. On the other hand, it has always been very difficult to implement due to all different situations that a human face can be found. Facial recognition is a form of computer vision that uses faces to attempt to identify a person or verify a person's claimed identity. Facial recognition includes five steps to complete their process (Figures 1–3).

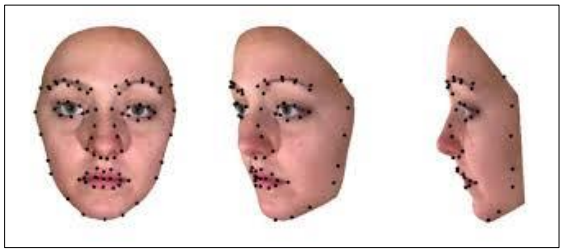

Fig. 1: *Acquire Image.*

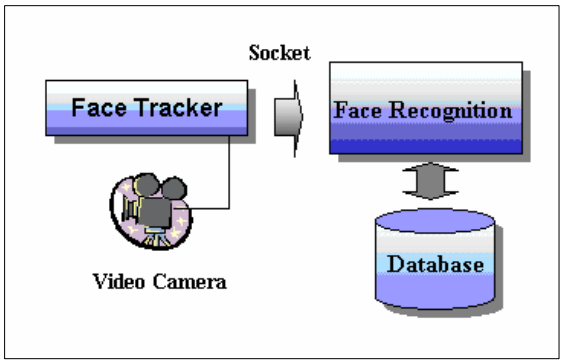

Fig. 2: *Process of Face Recognition System.*

Step1: Acquiring the image of an individuals face; Two ways to aquire image:

- Digitally scan an existing photograph;
- Acquire a live picture of a subject.

Step2: Locate image of face.

Software is used to locate the faces in the image that has been obtained.

Step3: Analysis of facial image.

Software measures face according to is peaks and valleys; focuses on the inner area of the face identified as the "golden triangle", valleys are used to create a face print with their nodal points.

Step4: Comparison.

The face print created by the software is compared to all face prints the system has stored in its database.

Step5: Match or No Match

Software decides whether or not any comparisons from step4 are close enough to declare a possible match.

Acquire Image	**Locate Face**	**Face Detection**	**Face Recognition**	**Person Identity**

Fig. 3: *Steps of Face Detection System.*

Facial recognition utilizes distinctive features of the face-including the upper outlines of the eye sockets, the areas surrounding the cheekbones, the sides of the mouth, and the location of the nose and eyes; to perform verification and identification.

Most technologies are fairly resistant to modest changes in haircut as they do not exploit areas of the face located near the hairline. When used in identification mode, facial recognition technology generally returns candidate lists of close matches as opposed to returning a single definitive match (as do fingerprint and iris-scan technologies).

Face Detection Problem Structure

Face detection is a concept that includes many sub-problems. Some systems detect and locate faces at the same time, others first perform a detection routine and then, if positive, they try to locate the face. Then, some tracking algorithms may be needed. Face detection algorithms usually share common steps. Firstly, some data dimension reduction is done, in order to achieve an admissible response; face detection algorithms usually share common steps.

Some pre-processing could also be done to adapt the input image to the algorithm prerequisites. Then, some algorithms analyze the image as it is, and some others try to extract certain relevant facial regions. The next phase usually involves extracting facial features or measurements. These will then be weighted, evaluated or compared to decide if there is a face and where is it. Finally, some algorithms have a learning routine and they include new data to their models.

Face detection is, therefore, a two class problem where we have to decide if there is a face or not in a picture. This approach can be seen as a simplified face recognition problem. Face recognition has to classify a given face, and there are as many classes as candidates. Consequently, many face detection methods are very similar to face recognition algorithms. Or put another way, techniques used in face detection are often used in face recognition (Figure 4).

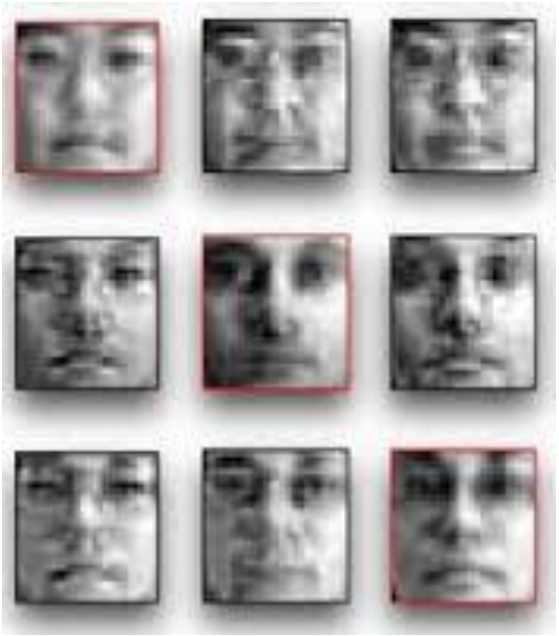

Fig. 4: *For Each Example in the Database We Add its Mirror Image and a Noisy Version.*

A New Appearance-Based Method

The templates in appearance-based methods are learned from the examples in the images. In general, appearance-based methods rely on techniques from statistical analysis and machine learning to find the relevant characteristics of face images. Some appearance-based methods work in a probabilistic network. An image or feature vector is a random variable with some probability of belonging to a face or not. Another approach is to define a discriminated function between face and non-face classes. These methods are also used in feature extraction for face recognition and will be discussed later. Nevertheless, these are the most relevant methods or tools:

Eigenface-Based

Sirovich and Kirby developed a method for efficiently representing faces using PCA (Principal Component Analysis). Their goal of this approach is to represent a face as a coordinate system. The vectors that make up this coordinate system were referred to as Eigen pictures. Later, Turk and Pent land used this approach to develop an Eigenface-based algorithm for recognition. ***Distribution-Based***

These systems where first proposed for object and pattern detection by Sung. The idea is

collect a sufficiently large number of sample views for the pattern class we wish to detect, covering all possible sources of image variation we wish to handle.

Then an appropriate feature space is chosen. It must represent the pattern class as a distribution of all its permissible image appearances. The system matches the candidate picture against the distribution-based canonical face model. Finally, there is a trained classifier which correctly identifies instances of the target pattern class from background image patterns, based on a set of distance measurements between the input pattern and the distribution-based class representation in the chosen feature space. Algorithms like PCA or Fisher's discriminate can be used to define the subspace representing facial patterns.

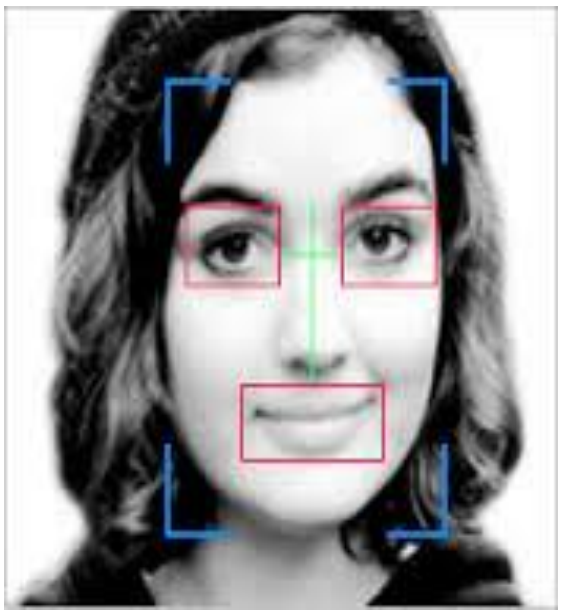

Fig. 5: *Face Tracking Process.*

Face Tracking

Many face recognition systems have a video sequence as the input. Those systems may require being capable of not only detecting but tracking faces. Face tracking is essentially a motion estimation problem (Figure 5). Face tracking can be performed using many different methods, e.g., head tracking, feature tracking, image-based tracking, model-based tracking. These are different ways to classify these algorithms:

Head Tracking/Individual Feature Tracking

The head can be tracked as a whole entity, or certain features tracked individually.

2D/3D

Two dimensional systems track a face and output an image space where the face is located. Three dimensional systems, on the other hand, perform a 3D modeling of the face. This approach allows estimating pose or orientation variations. The basic face tracking process seeks to locate a given image in a picture. Then, it has to compute the differences between frames to update the location of the face. There are many issues that must be faced: partial occlusions, illumination changes, computational speed and facial deformations.

The state vector of a face includes the center position, size of the rectangle containing the face, the average color of the face area and their first derivatives. The new candidate faces are evaluated by a Kalman estimator. In tracking mode, if the face is not new, the face from the previous frame is used as a template. The position of the face is evaluated by the Kalman estimator and the face region is searched around by a SSD algorithm using the mentioned template. When SSD finds the region, the color information is embedded into the Kalman estimator to exactly confine the face region. Then, the state vector of that face is updated. The result showed robust when some faces overlapped or when color changes happened.

Face Classification Algorithm

This approach is intuitive and simple. Patterns that are similar should belong to the same class. This approach has been used in the face recognition algorithms implemented later. The idea is to establish a metric that defines similarity and a representation of the same-class samples. Some classifiers are building based on a probabilistic approach. Bayes decision rule is often used. The rule can be modified to take into account different factors that could lead to miss-classification. Bayesian decision rules can give an optimal classifier, and the Bayes error can be the best criterion to evaluate features. Therefore, a posteriori probability functions can be optimal. There are different Bayesian approaches. One is to define a Maximum A Posteriori (MAP) decision rule.

$p(Z|wi)P(wi)=max\{p(Z|wj)P(wj)\}Z2wi$

Where wi are the face classes and Z an image in a reduced PCA space. Then, the within class densities (probability density functions) must be modeled. The covariance matrices are identical and diagonal, getting the components by sample variance in the PCA subspace. Other option is to get the within class covariance matrix by diagonal zing the within class scatter matrix using singular value decomposition (SVD). There are other approaches to Bayesian classifiers. Proposed on an alternative to the MAP-the maximum likelihood (ML). They proposed a non-Euclidean measure similarity measure, and two classes of facial image variations: Differences between images from the same individual (I, interpersonal) and variations between different individuals (E). This algorithms estimate the densities instead of using the true densities. These density estimates can be either parametric or nonparametric. Commonly used parametric models in face recognition are multivariate Gaussian distributions, as in. Two well-known non-parametric estimates are the k-NN rule and the Parzen classifier. They both have one parameter to be set, the number of neighbors k, or the smoothing parameter (bandwidth) of the Parzen kernel, both of which can be optimized. Moreover, both these classifiers require the computation of the distances between a test pattern and all the samples in the training set. These large numbers of computations can be avoided by vector quantization techniques, branch-and-bound and other techniques.

CONCLUSIONS

Face detection technology is very costly and top secure application. 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. Several results on face recognition and gender classification are presented, in which highly competitive recognition accuracies are achieved with a small number of features. The feature extraction can be applied to WT representation of images to provide a multi scale discriminate framework. In such cases the system becomes more complex at the expense of improving reparability and performance. The proposed feature extraction combined with soft classification seems to be a promising alternative to other face-recognition systems. We have developed a real time face recognition system by combining face tracking and face technologies together. The system has provided a platform for developing new face recognition algorithms. We are currently working on improving face recognition accuracy by a sequence of video images.

REFERENCES

1. Zhao W, Chellappa R, Nandhakumar N. Empirical Performance Analysis of Linear Discriminant Classifiers. *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*. 1998; 164–169p.
2. Yang J, Frangi AF, Yang J-Y, *et al.* KPCA Plus LDA: A Complete Kernel Fisher Discriminant Framework for Feature Extraction and Recognition. *IEEE Trans Pattern Anal Mach Intell*. 2005; 27(2): 230–244p.
3. Mika S, Rätsch G, Weston J, *et al.* Constructing Descriptive and Discriminative Nonlinear Features: Rayleigh Coefficients in Kernel Feature Spaces. *IEEE Trans Pattern Anal Mach Intell*. 2003; 25(5): 623–628p.
4. Wu X-J, Kittler J, Yang J-Y, *et al.* A New Direct LDA (D-LDA) Algorithm for Feature Extraction in Face Recognition. *Proc. International Conf. Pattern Recognition*. 2004; 4: 545–548p.
5. Jian H, Yuen PC, Wen-Sheng C. A Novel Subspace LDA Algorithms for Recognition of Face Images with Illumination and Pose Variations. *Proc. Int Conf. Machine Learning and Cybernetics*. 2004; 6: 3589–3594p.
6. Nefian AV. Embedded Bayesian Networks for Face Recognition. *Proc. of the IEEE Int Conf. Multimedia and Expo*; Lusanne, Switzerland. 26–29 Aug 2002; 2: 133–136p.
7. Mian Zhou, Hong Wei, Stephen Maybank. Gabor Wavelets and AdaBoost in Feature Selection for Face Recognition. *Workshop in Application of Computer Vision*. 2006.

8. Wenchao Zhang, Shiguang Shan, Xilin Chen, *et al.* Local Gabor Binary Patterns Based on Mutual Information for Face Recognition. *Int J Image Graph.* 2007.

AUTHOR BIUBLIOGRAPHY

P. Priya is assistant professor in computer science department at AVS college of arts & science. She completed her MCA and M.Phil. at Vivekananda Institute of Engineering and Technology, Anna University, Coimbatore. India. She finished her master of philosophy at Sri Sarada College for women (autonomous.) Area of interest include ImageProcessing, Pattern recognition, and software testing.

Cite this Article
Priya P. Detection System in Human Face using Biometrics. *Journal of Artificial Intelligence Research & Advances.* 2015; 2(3): 9–16p.