

A Case Study on Face Recognition Techniques

D.Sai Sirisha

Department of ECM,
K.L University, A.P, India.

P.CH.B.Sruthi

Department of ECM,
K.L University, A.P, India.

G.Subhramanya Sarma

Asst.Prof,
Department of ECM,
K.L University, A.P, India.

Abstract:

Recently face recognition is attracting much attention in the society of network multimedia information access. Areas such as network security, content indexing and retrieval, and video compression benefits from face recognition technology because “people” are the center of attention in a lot of video. Network access control via face recognition not only makes hackers virtually impossible to steal one’s “password”, but also increases the user-friendliness in human-computer interaction. Indexing and/or retrieving video data based on the appearances of particular persons will be useful for users such as news reporters, political scientists, and moviegoers.

For the applications of videophone and teleconferencing, the assistance of face recognition also provides a more efficient coding scheme. In this paper, we give an introductory course of this new information processing technology. The paper shows the readers the generic framework for the face recognition system, and the variants that are frequently encountered by the face recognizer. Several famous face recognition algorithms, such as eigen faces and neural networks, will also be explained.

Keywords:

face recognition ,eigen faces, techniques.

I.Introduction:

Face, the foremost distinguishing feature of human body, making you the ‘unique you’, not only gives you an individual identity, but can also save you from security breaches and fraud transactions, can take care of your personal data, and prevent your PC, wireless network from plausible security threats!! Unlike the world of facebook, where you can wear different face every day, here it is the uniqueness of your face that makes all the difference.

The fast track technology has brought the world at your finger tips, be it anything, it is not more than a click away. The easier life is getting day by day, the more complex it is becoming to escape from the traps intended to crack and get access to your private data. The growth of e-commerce wholly depends on the integrity of transaction.

The reason why a big percentage of people are still hesitant to employ e-commerce is the increasing cases of fraudulent fund transfer, loss of privacy and misuse of identity. End-to-end trust is must for its success. The ubiquitous methods of user id and password combinations, access cards are no longer free from security threats. Such scenario demands an infallible solution, the one that cannot be hacked, shared or stolen and that solution is present with us, as an innate gift of nature, the human biological characteristics.

BIOMETRICS:

‘Biometrics’ is the study of measurable biological characteristics. It consists of several authentication techniques based on unique physical characteristics such as face, fingerprints, iris, hand geometry, retina, veins, and voice. ‘Face recognition’ is a computer based security system capable of automatically verifying or identifying a person. It is one of the various techniques under Biometrics. Biometrics identifies or verifies a person based on individual’s physical characteristics by matching the real time patterns against the enrolled ones.

The quest of human minds to excel and explore the breathtaking possibilities that technology can meet, encouraged scientists in mid 1960s to teach computers to distinguish between faces. In its initial stage, the technique was semi automated. standard linear algebra technique, ‘Principle Component analysis’ that reduced the computation to less than a hundred values to code a normalized face.

II. WORKING:

When you face a security check based on face recognition, a computer takes your picture and after a few moments, it declares you either verified or a suspect. Let us look into the inside story, which is a sequence of complex computations. The process of recognition starts with Face detection, followed by normalization and extraction which leads to the final recognition. Face Detection: Detecting a face, an effortless task for humans, requires vigilant efforts on part of a computer. It has to decide whether a pixel in an image is part of a face or not. It needs to detect faces in an image which may have a non uniform background, variations in lightning conditions and facial expressions, thus making the task a complex one. The task is comparatively easy in images with a uniform background, frontal photographs and identical poses, as in any typical mug shot or a passport photograph. Traditionally, methods that focus on facial landmarks (such as eyes), that detect face-like colors in circular regions, or that use standard feature templates, were used to detect faces.

Normalization:

The detected facial images can be cropped to obtain normalized images called canonical images. In a canonical face image, the size It required an administrator to calculate the distance and ratios of various features of face (eyes, nose, ears and mouth) from a reference point and compare it with the images in database. Later in 1970s, Goldstein, Harmon and Lesk tried to automate the process by using various specific subjective markers such as lip thickness, hair color. Early approaches were cumbersome, as they required manual computations. However, it was in 1988, when Kirby and Sirovich used a image and in 1991, scientists finally succeeded in developing real time automated face recognition system. and position of the face are normalized approximately to the predefined values and the background region is minimized. Also, the image must be standardized in terms of size, pose, illumination, etc., relative to the images in the gallery or reference database. For this purpose, it is necessary to locate the facial landmarks accurately and failing to do so can make the whole recognition task unsuccessful. Recognition can only succeed if the probe image and the gallery images are the same in terms of pose orientation, rotation, scale, size, etc and normalization is meant to achieve this goal.

Extraction & Recognition normalized image can be processed further for feature extraction and recognition. Here, the images are converted to a mathematical representation, called biometric template or biometric reference, to store them into the database. These image database, then serves for verification and identification of probe images.

This transformation of image data to mathematical representation is achieved through algorithms. Many Facial recognition algorithms have been developed to get simplified mathematical form, to carry out the task of recognition. The way the algorithms transform or translate the image data which is in form of gray scale pixels to the mathematical representation of features, differentiate them from one another. To retain maximum information in the transformation process and thus create a distinct biometric template is crucial for successful recognition. Failing to which, may cause problems like generation of biometric doubles i.e. the biometric templates from different individuals become insufficiently distinctive.

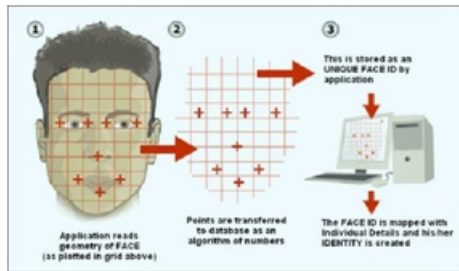
III. Algorithms:

Algorithms vary in the process of transformation (feature extraction) and matching (recognition). According to present developments algorithms are classified as Image based and Video based. Research is going on for the video based approach that enables recognizing humans from real surveillance videos.

The traditional predominant algorithms are based on either of the two basic approaches namely,

- Geometric (feature based)
- Photometric (view based)

The geometrical approach is based on geometrical relationship between facial landmarks, or in other words the spatial configuration of facial features. That means that the main geometrical features of the face such as the eyes, nose and mouth are first located and then faces are classified on the basis of various geometrical distances and angles between features. The limitation of this approach is that it is entirely based on detection of the landmarks, which may be difficult in case of pose variations, shadows and varying illumination.



On the other hand, the pictorial approach is based on the photometric characteristics of image. The method employs the templates of the major facial features and entire face to perform recognition on frontal views of faces.

Apart from these two techniques we have other recent template-based approaches, which form templates from the image gradient, and the principal component analysis approach, which can be read as a sub-optimal template approach. Finally we have the deformable template approach that combines elements of both the pictorial and feature geometry approaches and has been applied to faces at varying pose and expression.

IV. Techniques:

1. Principle Component Analysis (PCA):

PCA, the technique introducing the concept of 'Eigen faces', converts two dimensional vectors into one dimensional vectors, that can be decomposed into orthogonal components (eigen faces). It extracts the features of face which vary the most from rest of the image, in this way insignificant data is discarded and what remains is the most effective low dimensional facial structure pattern. Now, each face image can be represented as weighted sum (feature vector) of eigen faces and can be stored in a one dimensional array. A probe image is then compared against a gallery image by measuring the distance between their respective feature vectors.

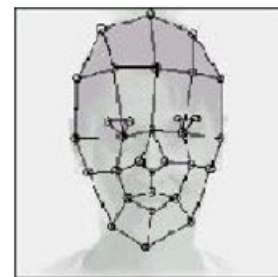
DRAWBACKS IN PCA:

PCA is reasonably sensitive to scale variations and hence the probe and gallery image must be of same size and should be normalized to line up the features within the image. Also, the pose and illumination variation between the two images is not acceptable.

2. Linear Discriminate Analysis(LDA):

LDA is based on same statistical principles as PCA. It classifies faces of unknown individuals based on training sequence of known individuals. The technique maximizes the variation between classes (different individuals) and minimizes variations within classes (samples of same person in varying pose, illumination). Showing variation between and within 6 classes using LDA. The algorithm thus, discriminates between individuals and at the same time can recognize image of same individual with some minor variations of expression, rotation and lightning.

3.1 Elastic Bunch Graph Matching (EBGM):



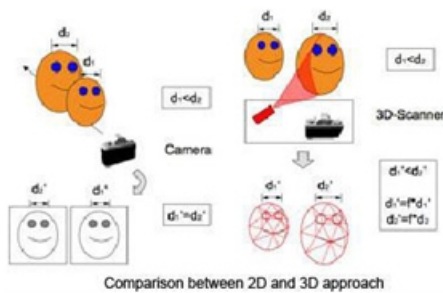
This technique is free from the limitations such as there should be no variations in illumination, pose angle, expression and contrast. The technique with its new approach considers non linear characteristics of face image such as pose variation (straight or leaned), lighting variations (outdoor or indoor) and expression variation. In this method, projection of face is made onto an elastic grid using a dynamic link architecture created by 'Gabor wavelet transform'. A node on elastic grid, called as 'Gabor jet', describes the behavior of image around the given pixel. Convolution of image with Gabor filter is done to extract features using image processing. The degree of similarity of Gabor filter response at each Gabor node is the basis of recognition. Accurate location of landmarks is must for this method. variations within classes (samples of same person in varying pose, illumination).



Showing variation between and within 6 classes using LDA.

3.2 2D to 3D:

Various limitations of 2D face recognition paved path for the emerging 3D facial recognition techniques. 2D face recognition techniques are sensitive to external factors such as varying illumination, pose and even to the use of cosmetics. Moreover, they require good quality of image. Also it should be a frontal image and these criteria must be met for both the probe and the gallery image. Further, there are even chances of security breach as the computer can be fooled by a printout picture in front of camera.



The 3D face recognition techniques use the 3D geometry of face for accurate identification. The distinctive features such as curves of eye socket, chin, nose, rigid tissues and bones are used. Also, the depth and axis measurement utilized is invariant of lightning changes. In the process of 3D facial recognition, the first stage is capturing of 3D image:



A structured light pattern gets distorted by the face geometry and the camera can record the distortion.

Measurement:

3D reconstruction algorithm is used to create the 3D mesh of the face. The curves of the face are then measured on a sub-millimeter scale.

Template formation:

A unique template based on the measurement is formed. Various algorithms translate the template into a set of codes, unique to the picture. This numeric template is stored in the database.



Verification and Identification: The stored images are matched for verification or identification purpose. For verification, only a 1:1 comparison needs to be done while for identification, the software needs to check the probe image with images in database till a match is found. The ongoing research is opening far more possibilities in 3D recognition. The 3D Isometric model for facial recognition is an expression invariant 3D recognition technique.

V.APPLICATIONS :

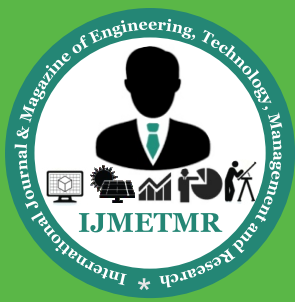
The innovative research going on in face recognition technology is resulting in the development of more sophisticated approaches every day. Along with the techniques, the applications too are increasing. Leading applications include restricting access to physical resources such as buildings and facilities and nowadays it has been extended for the way in to a country too!!

The US government has started 'US-VISIT' (United States Visitor and Immigrant Status Indicator Technology), aimed at foreign travelers gaining entry to the United States. The biometrics and photograph taken at the time of issuing visa are verified when the person arrives in US.

Controlling access to IT resources, such as computers and networks is one of the crucial applications. Unlike the use of proxy-type credentials such as cards, passwords or PINs, which can be easily shared or stolen, this solution confirms that the intended user was present for an access transaction.

As the system is becoming compatible with the cameras and computers already installed at various facilities like airports, banks etc, it is getting more popular for security at outdoor public spaces.

Many potential applications include national security, ATM and check cashing, counter terrorism, authentication for entry to secured high risk places like nuclear power plants, military bases and borders.



VI. Conclusion:

Face recognition is a 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.

VII.FUTURE SCOPE :

The admirable potential of facial recognition also has some drawbacks such as limited accuracy and highly complex and expensive installation. But the continuing advances in technology are showing potential to enhance the usability and limiting all limitations.

Face recognition, also considered as better than the rest of the Biometrics techniques, is an active research area involving integration of different fields such as physics, biology, mathematics, computer science and is presenting incredible solutions with the unified efforts. Hopes are high, to witness entirely secure and robust surroundings, scrutinized by our own face.

References:

- 1 .Belhumeur, P., hespanha, J., and Kriegman, D., "Eigenfaces vs. Fisher-faces: Recognition Using Class Specific Linear Projection", IEEE Trans. Pattern Analysis Machine Intelligence, vol. 19, no.7, pp.711-720, July 1997.
2. Brunelli, R., and Poggio, T., "Face Recognition: Features versus Templates", IEEE Trans. Pattern Anal. Machine Intell., vol. 15, pp.1042-1052, 1993.