INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Liveness Detection in Face Recognition Using Euclidean Distances

Annu[1], Dr. Chander Kant[2]

[1]M. Tech. Student, Deptt of Computer Science and Applications K.U.,
Kurukshetra, Haryana, INDIA
annu287@ymail.com

[2]Assistant Professor,Department of computer Science and Applications K.U.,
Kurukshetra, Haryana, INDIA
ckverma@reddifmail.com

Abstract: *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 ways is to do this by comparing the selected facial features from the image and a facial database but the main difficulty with this method is that the facial features may be fake and illegally used and that is a crucial weakness of the biometric system. In this paper, the proposed work includes a scheme which ensures that an input image actually originates from a live user instead of photograph or any other artificial sources. The proposed approach is based upon liveness detection technique which uses the concept of Euclidean distance test.*

Keywords: *Euclidean distance test, face recognition, facial database, facial features, liveness detection.*

1. INTRODUCTION

Face recognition systems are part of facial image processing applications and their significance as a research area are increasing recently. These systems use biometric information of the humans and are applicable easily instead of fingerprint, iris, signature etc., because these types of biometrics are not much suitable for non-collaborative people. These systems can be used for crime prevention, video surveillance, person verification, and similar security activities [1]. It is a combination of face detection and recognition techniques in image analysis. Detection application is used to find position of the faces in a given image [2].Numerous techniques have been developed to detect faces in a single image[3][4]. Recognition algorithm is used to classify given images with known structured properties, which are used commonly in most of the computer vision applications. These images have some known properties like; same resolution, including same facial feature components, and similar eye alignment. These images will be referred as "standard images" [5]. Face recognition algorithms try to solve the problem of both verification and identification [6].Recognition applications uses standard images, and detection algorithms detect the faces and extract face images which include eyes, eyebrows, nose, and mouth. Then, standard statistical pattern recognition techniques and/or neural network approaches are employed for matching faces using these measurements [7].

The process of face recognition is usually divided into five steps:

1: Image acquisition: image acquisition step captures the images of a face including the front profile, left profile or the right profile of the same person. Image acquisition is usually done using the CCD camera.

2: Detection: Detection of a face**:** this step is used to find the position of faces in a given image. Face detection performs locating and extracting face image operations for face recognition system. Output of the detection can be the location of face region as a whole, and location of face region with facial features (i.e. eyes, mouth, eyebrow, nose etc.).

3: Normalization: Normalization create the dimensionality consistent representation of the face image and also eliminate the non- face objects in the images to save the computation time.

*4: Feature extraction***:** this stage is used for extracting the information that can be used to distinguished different subjects, creating a template that represents the most discriminate features of the face. Some filtering operations are applied to extract feature candidates and steps are listed below:

- Laplacian of Gaussian Filter on Red channel of candidate.
- Contrast correction to improve visibility of filter result.
- Average filtering to eliminate small noises.

5: Matching: Matching the features vectors are compared using a similarity measure.

Finally, a decision of high confidence level is made to identify whether the user is an authentic or not. But here, the main problem is that we are not able to distinguish

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

between a dummy/fake image and a real image. An illustration of the steps for the face recognition system is given in figure 1.

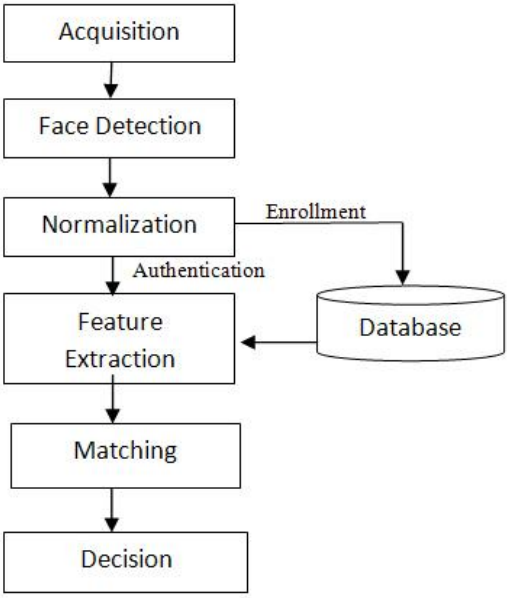

Figure 1: Techniques used in face recognition

1.1 SPOOFING IN BIOMETRIC SYSTEM

Attacker can attack any of the above mentioned stage for unauthorized access to the system; some of those attacks are like biometric sensor attack which happens at the beginning of the process. In this type of attack fake biometric data like artificial finger, a mask over a face or a contact lens on an eye etc. may be presented to the sensor and puts previously stored genuine biometric information into proper place in the processing chain. Following are some attacks that can be happen on biometric system [8].

- Fake biometric data at sensor: In this type of attack fake biometric trait like fake gummy finger, an iris printout or a face mask is used for unauthorized access.
- Resubmitting previously stored digitized biometric signals (replay attack). A digitized biometric signal, which has been previously enrolled and stored in the database, is again send to the system.
- Tampering biometric feature: In this attack extracted features of given biometric trait changed so that it can be accepted by matcher.
- Attack on enrollment: An enrollment database used in the verification/identification process can also be altered like by providing fake biometric traits.

These are some common attack mainly happened on biometric system. Some of attack can be resolved by maintaining some security like securing database from alteration. But some attacks like fake biometric data to the sensor cannot be covered by strong security. So, for this type of attacks liveness detection technique is used to ensure that the given biometric sample originates from a living person and is not artificial.

2. RELATED WORK

Traditional recognition systems have the abilities to recognize the human using various techniques like feature based recognition, face geometry based recognition, classifier design and model based methods. There are three most popular appearance-based face recognition projection methods (PCA, LDA and ICA). Principal Components Analysis (PCA) was firstly used by Sirovich and Kirby [12], which were latterly adopted by M. Turk and A. Pentland introducing the famous idea of eigenfaces [13-14]. Using PCA [9], a face subspace is constructed to represent "optimally" only the face object. Using LDA [10], a discriminate subspace is constructed to distinguish "optimally" faces of different persons. In comparison with PCA which takes into account only second order statistics to find a subspace, ICA [11] captures both second and higher order statistics and projects the input data onto the basis vectors that are as statistically independent as possible. Model-based techniques consist of four components: the model, the initialization algorithm, the objective function, and the fitting algorithm. The model contains a parameter vector **p** that represents its possible configurations, such as position, orientation, scaling, and deformation. Models are mapped onto the surface of an image via a set of feature points, a contour, a textured region, etc. Deformable models are highly suitable for analyzing human faces with all their individual variations. The type of models using shape and texture parameters is called Active Appearance Models (AAMs). Another technique is 3-D Model-Based Technique. In this technique, The main argument in favor of using 3D information for face recognition appears to be that it allows us to exploit features based on the shape and the curvature of the face (such as the shape of the forehead, jaw line, and cheeks) without being plagued by the variances caused by lighting, orientation and background clutter that affect 2D systems. Feature-based approaches first process the input image to identify and extract (and measure) distinctive facial features such as the eyes, mouth, nose, etc., as well as other facial marks, and then compute the geometric relationships among those facial points, thus reducing the input facial image to a vector of geometric features. Standard statistical pattern recognition techniques are then employed to match faces using these measurements. The detection of faces and their features prior to performing verification or recognition makes these approaches robust to positional variations of the faces in the input image. Another well-known feature-based approach is the elastic bunch graph matching method proposed by Wiskott et al. [15]. This technique is based on Dynamic Link Structures [16]. The main advantage offered by the featured-based techniques is that since the extraction of the feature points precedes the analysis done for matching the image to that of a known individual, such methods are relatively robust to position

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

variations in the input image. The major disadvantage of these approaches is the difficulty of automatic feature detection.

3. PROPOSED FACE RECOGNITION ALGORITHM FOR IMAGE ACQUISITION

3.1 Architecture of the proposed approach

A block diagram of the proposed face recognition system is shown in figure 2.

The architecture of the proposed approach is divided into two steps:

1. *Enrollment*: User enrollment is a process that is responsible for registering individuals in the biometric system storage. During the enrollment process, the biometric characteristics of a person are first captured by a biometric scanner to produce a sample. Some systems collect multiple samples of a user and then either select the best image or fuse multiple images or create a composite template. Then the Euclidean distance test is performed to check the liveness of a person. If the person is live then the enrollment process takes the enrollment template and stores it in the system storage along with the demographic information about the user.
2. *Authentication*: In this process, the subject does not explicitly claim an identity and the system compares the feature set against the templates of all the subjects in the system storage; the output is a candidate list that may be empty or contain one or more identifiers of matching enrollment templates.

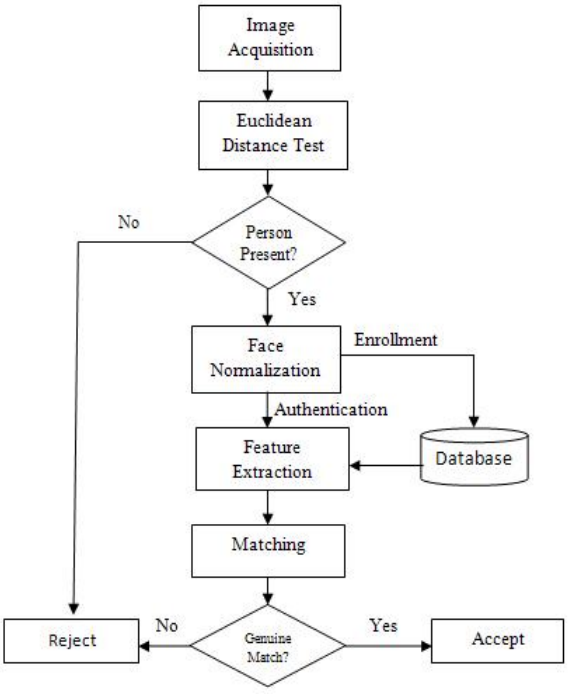

Figure 2: Architecture of the proposed approach

***The modules of the proposed approach are explained as follows*:**

1. *Image Acquisition*: An important and complex step of face recognition is image acquisition of a very high quality of a person. It is difficult to acquire clear images using the standard CCD camera with ordinary lighting. In this module, a biometric camera is used to capture the user's face images. The image acquisition phase should consider three main aspects, that is to say, the lighting system, the positioning system, and the physical capturing system. The face recognition system can work both in outdoor and indoor conditions without any hot spot of lighting intensities.
2. *Euclidean Distance Test*: This module is used for checking the person's liveness and is further described in the section 3.2.
3. *Face Normalization*: Create the dimensionality consistent representation of the face image and also eliminate the non- face objects in the images to save the computation time.
4. *Feature Extraction*: This stage is used for extracting the information that can be used to distinguish different subjects, creating a template that represents the most discriminant features of the face. This is done with the help of the PCA technique.
5. *Matching*: This stage takes a feature set and an enrollment template as inputs and computes the similarity between them in terms of a matching score. The matching score is compared to a system threshold to make the final decision; if the match score is higher than the threshold, the person is recognized, otherwise not.

3.2 Euclidean distance test

Biometric features may be fake and illegally used. This is a crucial weakness of the biometric system. This section aims to ensure that an input image actually originates from a user instead of face photographs or any other artificial sources. In the proposed work, Euclidean distance test is suggested to overcome this problem. So, here we use the concept of Euclidean distance.

3.2.1 Euclidean distance

Euclidean distance between two points in p-dimensional space is a geometrically shortest distance on the straight line passing through both the points[17].

For a distance between two p-dimensional features x=(x1,x2,……,xp) and y=(y1,y2,……yp) the Euclidean distance is defined as follows:

$$d(x,y)=[\quad x_i-y_i)^2]^{1/2}$$

So, if the images are of the same person then their Euclidean distance should be minimum otherwise they come from the different sources.

3.2.2 Algorithm of the proposed approach

The algorithm of this method is elaborated as follows:

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Step 1: Capture the same person's face images under the three different profiles- left, right and front (at least one from each profile) in any random order. For example, LRF or it may be FLR etc.
Step 2: Measure the Euclidean distance from the captured face images. If these values are dissimilar then the image is actually coming from a real source (user), otherwise artificial sources may have been used.

Euclidean distance is given by:
$d(x,y)=\{ \quad x_i-y_i)^2\}^{1/2}$ (1)
Using eq'n (1), we can calculate the difference between the Euclidean distances of the two different images of the same person.

$T_d= \quad d(x_i,y_i)-d(x_{i+1},y_{i+1})|$ (2)

EDT= (3)

Here, EDT is the euclidean distance test parameter, n is the no of face images taken in any of the following order i.e., it may be LFR, LRF, FLR, RLF, RFL, FRL whereas L denotes the left profile and R denotes the right profile and F denotes the front profile of a person. $d(x_i,y_i)$ and $d(x_{i+1},y_{i+1})$ are also the Euclidean distance of the person under different profiles. T_d is the difference between the Euclidean distances of the two images. If the T_d is not equal to zero that means the person image is real and not coming from a fake biometric system or any other artificial sources and responding to euclidean distance test.

3.2.3 Comparison

The proposed work presents a technique for liveness detection which uses the concept of Euclidean distance. This technique ensures the detection of fake/dummy images and also verifies that the person is actually alive or not. But the traditional method does not use the concept of Euclidean distance. Therefore, this method is not able to check that the person is actually alive or not. May be the person's image is fake or generated from artificial sources. The main advantage of the proposed work is that if the person is found fake then it is detected in the euclidean distance test module and the further computations are not done. But in the traditional method, there is no provision for liveness detection and thus it was not able to detect the liveness of the person.

4. CONCLUSION AND FUTURE WORK

Euclidean distance test (EDT) is used for checking a person's aliveness which ensures the detection of fake/dummy images. The proposed liveness detection approach not only verifies that the given biometric sample is from an authorized person but also verifies that the given biometric sample is real or fake. Initially, it checks the liveness of the person. If the person is found alive, only then the further calculations are performed. This proposed approach is suitable for any real time applications such as e-voting, employee management, terrorist identification, passport verification etc. EDT opens a new path in face recognition research work. In further development, this system can be improved to identify a person at a few meters distance.

REFERENCES

[1] **R. Chellappa, C. L. Wilson and S. Sirohey, "Human and Machine Recognition of Faces: A Survey", Proceedings of the IEEE, Vol. 83, No. 5, May 1995.**
[2] **Wang, C., and Brandstein, M.S., "A hybrid real-time face tracking system" *Proc. ICASSP 1998*, Seattle, WA, May, 1998, pps. 3636-3740.**
[3] **A. King, "A survey of methods for face detection," Technical Report. McGill Unv., Mar. 2003.**
[4] **M. Yang, D.J. Kriegman and N. Ahuja, "Detecting faces in images: a survey," IEEE.**
[5] **J. Weng and D. L. Swets, "Face Recognition", in A. K. Jain, R. Bolle, and S. Pankanti (Editors), Biometrics: Personal Identification in Networked Society, Kluwer Academic Press,1999.**
[6] **S.A. Rizvi, P.J. Phillips, and H. Moon, "A verification protocol and statistical performance analysis for face recognition algorithms", pp. 833-838, IEEE Proc. Conf. Computer Vision and Pattern Recognition (CVPR), Santa Barbara, June 1998.**
[7] **Encoding and Back propagation Neural Network", pp. 159-161, 5th International Symposium on Signal Processing and P. Temdee, D. Khawparisuth, and K. Chamnongthai, "Face Recognition by Using Fractal its Applications, ISSPA '99, Australia, August 1999.**
[8] **Galbally, J., Fierrez, J., Ortega-Garcia, J.: Vulnerabilities in biometric systems: Attacks and Recent Advances in Liveness Detection, Biometrics Recognition Group, Madrid, Spain, 2007, p.8.**
[9] **Turk, M., Pentland, A.: Eigenfaces for Recognition, Journal of Cognitive Neurosicence, 3(1), 1991, 71–86.**
[10] **Zhao, W., Chellappa, R., Krishnaswamy, A.: Discriminant Analysis of Principal Components for Face Recognition,Proc. of the 3rd IEEE International Conference on Face and Gesture Recognition, FG'98, (1998) 336.**
[11] **Bartlett, M.S., Movellan, J.R., Sejnowski, T.J.: Face Recognition by Independent Component Analysis, IEEE Trans. on Neural Networks, 13(6), (2002) 1450–1464L. Sirovich and M.**
[12] **Kirby, "Low-dimensional procedure for the characterization of human faces", *J. Opt. Soc. Am. A, Vol. 4, No. 3*, March 1987, pp 519-524.**

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

[13] Turk M.A., Pentland A.P., "Face Recognition using Eigenfaces", *IEEE Conference on Computer Vision and Pattern Recognition*, 1991, pp 586-591.

[14] Turk M.A., Pentland A.P., "Eigenfaces for Recognition", *Journal of Cognitive Neuroscience* 3 (1): 1991, pp 71-86.

[15] L. Wiskott, J.-M. Fellous, N. Krüger, and C. von der Malsburg, "Face Recognition by Elastic Bunch Graph Matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol.19, pp.775- 779, 1997.

[16] M. Lades, J. C. Vorbrüggen, J. Buhmann, J. Lange, C. v. d. Malsburg, R. P. Würtz, and W. Konen, "Distortion invariant object recognition in the dynamic link architecture," *IEEE Trans. Computers*, Vol.42, pp.300-311, 1993.

[17] J. Li, G. Chen, and Z. Chi, "A Fuzzy Image Metric with Application to Fractal Coding," *IEEE Trans. Image Processing*, vol. 11, no. 6, pp. 636-643, June 2002.