

# A Survey on Face Recognition System used in Criminal Detection

<sup>1</sup>Prof.Rachana Mehta, <sup>2</sup>Prof. Vidushi Patel, <sup>3</sup>Prof. Nirmal Patel, <sup>4</sup>Prof. Namita Patel

<sup>1</sup>Assistant professor, <sup>2</sup>Assistant professor, <sup>3</sup> Assistant professor, <sup>4</sup> Assistant professor  
Aditya Silver Oak Institute of Technology& Science, Ahmedabad, India

**Abstract :** Human face detection by computer system has become a major field of interest. Face detection algorithms are used in wide range of applications such as a security control, video retrieving, biometric signal processing, human computer interface and many others. This report proposes a face detection system to detect abnormal activities and crime detection by use of face detection camera system. This system is connected through database. This method detect face over the entire image and then generate face candidates based on a connected component analysis. Finally the face candidates are divided into human face and non-face image and then it detect exceptional activities which help to our global system to reduce criminal activities and also help to detect skeptical person.

**Index Terms –** Face Recognition, Detection, Criminal Detection, Principle Component Analysis, Linear discriminate analysis

## I. INTRODUCTION

Facial recognition is a type of biometric software application that can identify a specific individual in a digital image by analyzing and comparing patterns. Facial recognition systems are commonly used for security purposes but are increasingly being used in a variety of other applications. Most current facial recognition systems work with numeric codes called face prints. Such systems identify 80 nodal points on a human face. In this context, nodal points are end points used to measure variables of a person's face, such as the length or width of the nose, the depth of the eye sockets and the shape of the cheekbones. These systems work by capturing data for nodal points on a digital image of an individual's face and storing the resulting data as a faceprint. The faceprint can then be used as a basis for comparison with data captured from faces in an image or video[1].

This face recognition system concept is used in identify criminals too. The process of uncovering criminal activity (or verifying reported crime).It is relying on artificial intelligence(AI) to automatically identify and detect problematic and criminal behavior as it happens. Cameras use a statistical method called machine learning to learn what is normal for an area and then alerts on abnormal activity[2].

## FACE RECOGNITION SYSTEM

### 1.1 BASIC WORKING PROCESS.

The face is an important part of who you are and how people identify you. For face recognition there are two types of comparisons. The first verification is where the system compares the given individual with their identity and gives a yes or no decision. The second is identification, where the system compares the given individual to all the other individuals in the database and gives a ranked list of matches [3].



All identification or authentication technologies operate using the following four stages:

- Capture: a physical or behavioral sample is captured by the system during enrollment and also in identification or verification process.
- Extraction: unique data is extracted from the sample and a template is created.
- Comparison: the template is then compared with a new sample.
- Match/non match: the system decides if the features extracted from the new sample are a match or a non-match[3].

Face recognition technology analyze the unique shape, pattern and Positioning of the facial features. Face recognition is very complex technology and is largely software based. This Biometric Methodology establishes the analysis framework with tailored algorithms for each type of biometric device[1].

## 1.2 USES OF SYSTEM.

A lot of facial recognition development is focused on smartphone applications. Smartphone facial recognition capacities include image tagging and other social networking integration purposes as well as personalized marketing. It can take a picture of an individual and within seconds return the individual's name, date of birth and social security number.

Facebook uses facial recognition software to help automate user tagging in photographs. How facial recognition works in Facebook is each time an individual is tagged in a photograph, the software application stores information about that person's facial characteristics. When enough data has been collected about a person to identify them, the system uses that information to identify the same face in different photographs, and will subsequently suggest tagging those pictures with that person's name[6].

Facial recognition software also enhances marketing personalization. For example, billboards have been developed with integrated software that identifies the gender, ethnicity and approximate age of passersby to deliver targeted advertising.

It is also used in identifying criminals and to prevent Criminal Activity before it happens for the safety purpose of civilians. For effective surveillance of criminal activity.

Utilizing content analysis and database techniques that can provide law enforcement with the means to effectively respond to criminal activity at scale[4].

## II. CRIMINAL DETECTION CAMERA SYSTEM

### 2.1 WHAT IS IT?

Criminal detection camera is not a simple video recording system but it is monitoring of the behavior activities of human beings, or other changing information, usually of people for the purpose of managing, directing, or protecting them and their activities done around them[1].

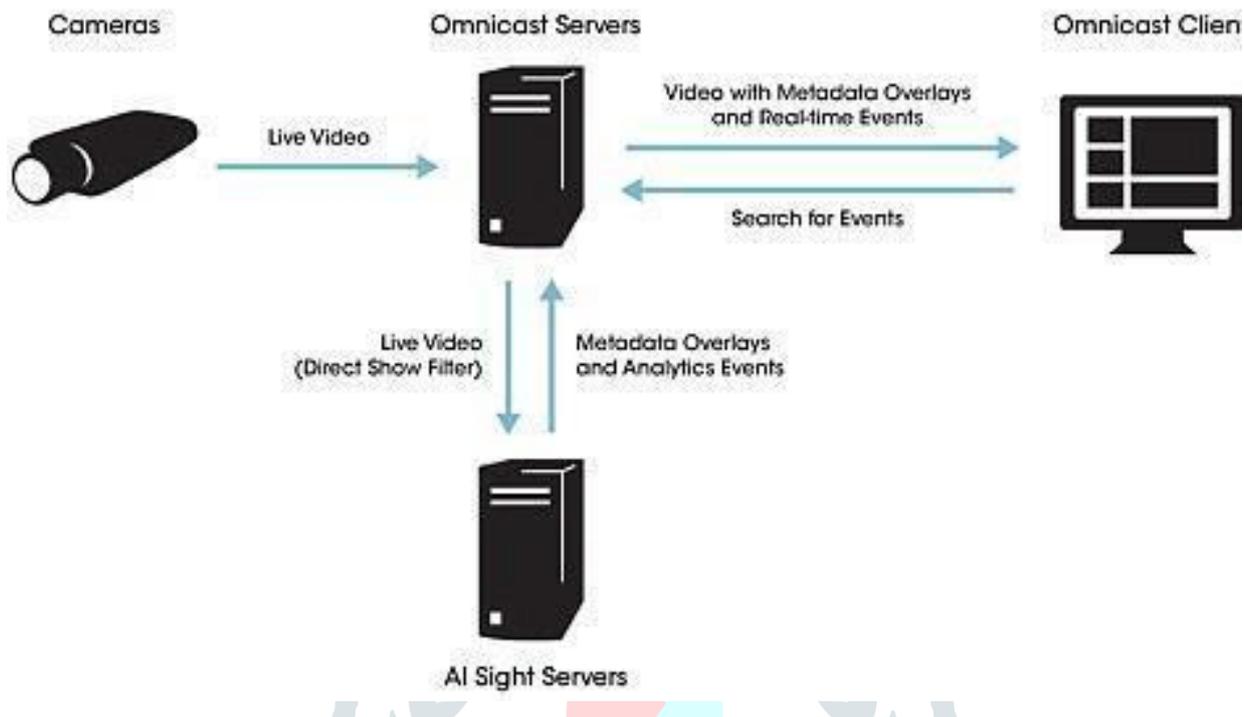
This can include observation from a distance by means of electronic equipment (such as CCTV cameras) and then analysis of footage has been made easier by automated software that organizes digital video footage into a searchable database. By that government should uncovering criminal activities. Generally cameras use a statistical method called machine learning to "learn what is normal for an area and then alerts on abnormal activity," according to its Behavioral Recognition System which made by its creator. Originally the systems were installed to deter burglary, assault and car theft but their use has been extended to include combating 'anti-social behavior' and it is discovered as form of criminal detection camera system. Camera images of offences can play an important role in investigations. This is evident from the government's investigative programs which make use of a selection of camera images. On the other hand, the business world and private individuals have widespread access to security cameras and smartphones.so this type of crime detection camera system is very essential for secure modern world in which criminal should play their roll with advanced system. The process of uncovering criminal activity (or verifying reported crime).It is relying on artificial intelligence(AI) to automatically identify and detect problematic and criminal behavior as it happens. Cameras use a statistical method called machine learning to learn what is normal for an area and then alerts on abnormal activity[2].

### 2.2 HOW IT WORKS?

Basically it is works on concept of face detection or face recognition technique. A facial recognition system is a computer application capable of identifying or verifying a person from a digital image or a frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. If you look at the mirror, you can see that your face has certain distinguishable landmarks. These are the peaks and valleys that make up the different facial features and there are about 80 nodal points on a human face[6].

Facial recognition software is based on the ability to first recognize faces, which is a technological feat in itself. Some facial recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For

example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation



Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features, or photometric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances[2].

Following are the few nodal points that measured by the software[2]:

1. Distance between the eyes
2. Width of the nose
3. Depth of the eye socket
4. Cheekbones
5. Jaw line
6. Chin

There are few steps of detecting face process are given below:

- **Detection**- when the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for faces. If there is a face in the view, it is detected within a fraction of a second. A multi-scale algorithm is used to search for faces in low resolution. The system switches to a high-resolution search only after a head-like shape is detected[3].
- **Alignment**- Once a face is detected, the system determines the head's position, size and pose. A face needs to be turned at least 35 degrees toward the camera for the system to register it[3].
- **Normalization**-The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose. Normalization is performed regardless of the head's location and distance from the camera. Light does not impact the normalization process[3].
- **Representation**-The system translates the facial data into a unique code. This coding process allows for easier comparison of the newly acquired facial data to stored facial data.

- **Matching-** The newly acquired facial data is compared to the stored data and (ideally) linked to at least one stored facial representation[3].
- The system maps the face and creates a faceprint, a unique numerical code for that face. Once the system has stored a faceprint, it can compare it to the thousands or millions of face prints stored in a database.
- Each faceprint is stored as an 84-byte file.
- It has the ability to leverage existing image equipment.
- It can search against static images such as driver's license photographs.
- It is the only biometric able to operate without user cooperation[3].

### 2.3 ALGORITHMS USED IN IT.

There are so many algorithms used in face detection or face recognition. Facial recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation.[4].

Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features, or photometric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances[4].

Popular recognition algorithms include principal component analysis using Eigen faces, linear discriminant analysis, elastic bunch graph matching using the Fisher face algorithm, the hidden Markov model, the multilinear subspace learning using tensor representation, and the neuronal motivated dynamic link matching[4]. A reliable face-detection approach based on the genetic algorithm and the Eigen-face technique.

1. Principal component analysis (PCA) is a statistical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables called principal components. If there are  $n$  observations with  $p$  variables, then the number of distinct principal components is  $\min(n-1, p)$ . This transformation is defined in such a way that the first principal component has the largest possible variance (that is, accounts for as much of the variability in the data as possible), and each succeeding component in turn has the highest variance possible under the constraint that it is orthogonal to the preceding components. The resulting vectors are an uncorrelated orthogonal basis set. PCA is sensitive to the relative scaling of the original variables.
2. Linear discriminant analysis (LDA) or discriminant function analysis is a generalization of Fisher's linear discriminant, a method used in statistics, pattern recognition and machine learning to find a linear combination of features that characterizes or separates two or more classes of objects or events. The resulting combination may be used as a linear classifier, or, more commonly, for dimensionality reduction before later classification. LDA is closely related to analysis of variance (ANOVA) and regression analysis, which also attempt to express one dependent variable as a linear combination of other features or measurements.[1][2] However, ANOVA uses categorical independent variables and a continuous dependent variable, whereas discriminant analysis has continuous independent variables and a categorical dependent variable (i.e. the class label).[3] Logistic regression and probit regression are more similar to LDA than ANOVA is, as they also explain a categorical variable by the values of continuous independent variables. These other methods are preferable in applications where it is not reasonable to assume that the independent variables are normally distributed, which is a fundamental assumption of the LDA method.

### 2.4 ADVANTAGES OF IT.

- To prevent Criminal Activity before it happens
- For the safety purpose of civilians.
- For effective surveillance of criminal activity.
- Utilizing content analysis and database techniques that can provide law enforcement with the means to effectively respond to criminal activity at scale[5].
- Face recognition is easy to use and in many cases it can be performed
- Without a person even knowing.
- Face recognition is also one of the most inexpensive biometric in the
- Market and its prices should continue to go down[3].

## 2.5 DISADVANTAGES OF IT.

Face recognition systems can't tell the difference between identical Twins [3].

1. Image quality: Image quality affects how well facial-recognition algorithms work. The image quality of scanning video is quite low compared with that of a digital camera. Even high-definition video is, at best, 1080p (progressive scan); usually, it is 720p. These values are equivalent to about 2MP and 0.9MP, respectively, while an inexpensive digital camera attains 15MP. The difference is quite noticeable[6].



Feature Extractor	No. of Images	FAR = FRR (%)	
		FAR	FRR
PCA	8	15	85
	12	17	83
	15	20	80
LDA	8	13	83
	12	12	88
	15	07	92.33

2. Image size: When a face-detection algorithm finds a face in an image or in a still from a video capture, the relative size of that face compared with the enrolled image size affects how well the face will be recognized. An already small image size, coupled with a target distant from the camera, means that the detected face is only 100 to 200 pixels on a side. Further, having to scan an image for varying face sizes is a processor-intensive activity. Most algorithms allow specification of a face-size range to help eliminate false positives on detection and speed up image processing[2].
3. Face angle: The relative angle of the target's face influences the recognition score profoundly. When a face is enrolled in the recognition software, usually multiple angles are used (profile, frontal and 45-degree are common). Anything less than a frontal view affects the algorithm's capability to generate a template for the face. The more direct the image (both enrolled and probe image) and the higher its resolution, the higher the score of any resulting matches [6].
4. Processing and storage: Even though high-definition video is quite low in resolution when compared with digital camera images, it still occupies significant amounts of disk space. Processing every frame of video is an enormous undertaking, so usually only a fraction (10 percent to 25 percent) is actually run through a recognition system. To minimize total processing time, agencies can use clusters of computers. However, adding computers involves considerable data transfer over a network, which can be bound by input-output restrictions, further limiting processing speed [1].

## 2.6 APPLICATION OF IT.

1. To prevent Criminal Activity before it happens
2. For the safety purpose of civilians.
3. For effective surveillance of criminal activity.
4. Utilizing content analysis and database techniques that can provide law enforcement with the means to effectively respond to criminal activity at scale[6].

## III. CONCLUSION

Because of increase in criminal activities, face detection system is a very essential now days. In criminal detection camera mainly based on face detection or face recognition system which is very complex and their have some limits in past days, but by using many advance technology like 2D and 3D face visualization system and other advance software available in market made it easy to use. It helps to reduce crime rate. Today the core technologies have evolved and the cost of equipments is going down grammatically due to integration and increasing processing power. Certain application of face recognition technology are now cost effective, reliable and highly accurate. As a result the uses of this system increase rapidly and these would help to reduce crime rate by observing abnormal activities.

## REFERENCES

1. NirmalyaKar, MrinalKantiDebbarna, AshimSaha, and DwijenRudra Pal," Study of Implementing Automated Attendance System Using Face Recognition Technique",in proc. International Journal of Computer and Communication Engineering, Vol. 1, No. 2, July 2012

2. Naveed Khan Balcoh, M. Haroon Yousaf, Waqar Ahmad and M. Iraam Balg, "Algorithm for efficient attendance management: face recognition based approach", in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012
3. Sarabjit Singh, Amritpal Kaur, Taqdir, A Face Recognition Technique using Local Binary Pattern Method, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2015.
4. Wright, J., Yang, A.Y., Ganesh, A., Sastry, S.S. and Ma, Y., 2009. Robust face recognition via sparse representation. IEEE transactions on pattern analysis and machine intelligence, 31(2), pp.210-227.
5. Wiskott, L., Krüger, N., Kuiger, N. and Von Der Malsburg, C., 1997. Face recognition by elastic bunch graph matching. IEEE Transactions on pattern analysis and machine intelligence, 19(7), pp.775-779.
6. Phillips, P.J., Wechsler, H., Huang, J. and Rauss, P.J., 1998. The FERET database and evaluation procedure for face-recognition algorithms. Image and vision computing, 16(5), pp.295-306.
7. Gottumukkal, R. and Asari, V.K., 2004. An improved face recognition technique based on modular PCA approach. Pattern Recognition Letters, 25(4), pp.429-436.

