Review on Digital Image Processing Techniques for Face Recognition

Yogalakshmi.S , Megalan Leo.L, Jerrin Simla.A

***Abstract*—In the world of advancement, security is an important aspect of everyone's life. Personal data is easily accessed by hackers. This kind of problem can be reduced by using biometric access. Fingerprint, voice recognition, iris recognition, face recognition, and dental data is the few biometric techniques that provide end to end security between the user and service provider. Digital image processing plays a major role in this biometric recognition technique. Advancement in the digital image processing technique with the intellectual computer allows the researcher to work on this recognition technique. All recognition techniques have its merit and demerits. Face recognition is the most preferred technique which is not only providing secure access and also helpful to limit unauthorized access. Nowadays, social sites are using this technique to identify the user. If one photo is uploaded on the website immediately it matches the images with the database and helps the user to tag their friends. Advanced applications help the user by capturing their mood and play the songs, images, and so on. In this work, the basic image processing techniques to advance image processing techniques in face recognition are presented in a meaningful way. It will be useful for beginners, and researchers who want to work in face recognition techniques.**

***Index Terms*—Secure Access, Face recognition, Artificial Intelligence, Image Processing**

I. Introduction

In the modern era, everything becomes digitized. In the earlier stage, passwords and keys were only used for providing secure access. Hackers find easy to steal the password and keys. Common passwords used by individuals can be easily hacked by presumption. Unauthorized access is a serious threat to the safety of individuals. Individuals may lose their valuable data such as account details, photos, emails, and personal details. The above problem leads to a serious threat to their personal life by accessing there computer or mobile as a gateway for doing some illegal activities.

In other cases, Hackers fail to guess the difficult password set by the individuals and companies. But lots of intelligent programs, running on the machine help them to know the password or key. So a week or strong Password is not sufficient to provide the security because they can be easily broken by advanced programming or simple guess. Biometric access increases the value of the security because it verifies the physical presence of the user. Fingerprints, iris, voice, and face are some of the biometric techniques used to provide security. In order to prevent users from unauthorized access biometric should be used in addition to the password. Now a day, in the working environment, the fingerprint is used for logging in to different secure processes such as network page and server room. Attendance is also calculated by the thump impression. Since passwords can be easily shared among the workers' biometric access completely avoids sharing and enhances security. Biometric security provides a lot of benefits to the individuals and management of different companies. Notebooks are used in the offices to register the attendance of the employees. But employees can able to sign for others if they know their signature. It affects the working environment. Instead of this, if an organization uses a password, then it can also be shared among employees. So only way to avoid the above problem and to increase the efficiency is by the use of fingerprint. Other advantages are strong authentication and impossible to duplicate. Though fingerprint provides many advantages, it has a major drawback of fooling. If a person decides to break then a fake finger can be created with plastic mold and gelatin. It can be used for logging in secure systems. Face recognition is the biometric technique that can overcome the above-said problem in an effective way. It is not only used to provide secure access also use to identify victims in various incidents. Facebook uses a face recognition technology to identify the friends of the user and also provide option to tag them. Intelligent programming with machines makes this task as efficient. Sometimes it is smarter than human beings. In human beings, the brain is responsible for the recognition of individuals based on the physical and behavioral changes of face, action, and voice. In the machine, artificial neurons are used as a learning parameter and it learns from the input by running an algorithm upon it. In the database, face images are stored. These data are given as input to the neural network. It learns different features from it. This technique called machine learning. In the face recognition system, if the user passes the camera then the image captures and it compared with the existing database. If it matches secure access can be provided. Otherwise, it passes a security threat message.

S.Yogalakshmi is working in the school of Electrical and Electronics Engineering in Sathyabama Institute of Science and Technology,Chennai. (e-mail: yogalakshmi1015@ gmail.com).

L.Megalan Leo is working in the school of Electrical and Electronics Engineering in Sathyabama Institute of Science and Technology,Chennai (Corresponding author: 9003567001, e-mail: megalanleo@gmail.com)

A.Jerrin Simla is working in the Department of Computer Science Engineering in Panimalar Institute of Technology,Chennai (e-mail: jerrinsimla@gmail.com)

978-1-7281-4988-2/20/$31.00 ©2020 IEEE

Face recognition systems are used in the following applications. The deep face is facing the recognition system developed by Facebook. It is an artificial network that comprises nine layers of neurons activated by 120 million connection weight. It is trained on four million images uploaded by Facebook users. It detects human faces with 97 percent accuracy. FaceNet is another artificial intelligent application developed by Google to recognize the persons by face recognition. It is trained on 260 million dataset images of faces from different parts of the world. It recognizes face with 86 percent accuracy. It also displays identical faces across the world. In immigration, a face recognition system is used to identify the fraudulent activities in passport and visa. A study in Australian passport shows that, face recognition techniques more efficient than people detecting fraud. It is also used in RTO offices for verifying the driving license. In China, face recognition techniques are used to increase the security of the card user. It uses face mapping and iris recognition.ATM and banks are used in this technique to prevent unauthorized access. Face recognition plays a major role in the investigation of crime. Several complicated cases are solved easily with the help of this technique. The advantage of this technique is the detection of faces from different angles. In, 2000 face recognition technology is used in Mexico to prevent fraud voters. Due to this fraud votes were avoided and it reduces the duplicate votes. It is also used as an attendance tracker in the various organizations. The employee needs to show their faces in the camera and the attendance will be given by matching with the database. The paper is organized as follows. Section II describes the review on face detection algorithms. At last, Section III concludes the paper with conclusion.

II. Review on Face Detection algorithms

Image processing generally does the pixel-wise transformation, It is a type of signal processing in which the source is an image and the destination may be image or characteristics/features connected with that image i.e mapping of an input image to the output image. The most commonly used image processing applications are used with face and character recognition, where specific characteristics within an input image are isolated by using the set of algorithms. The extraction of meaningful information from images is done through computer vision. A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source, face recognition is usually worked by comparing selected facial features from a given image with faces within the database [1]. The computer is developing more and more intellectually in a faster way. Face detection is the stepping stone to all facial analysis algorithms, including face alignment, face modeling, face relighting, face recognition, face verification/authentication, head pose tracking, facial expression tracking/recognition, gender/age recognition, etc. An original image received from various sources like satellites, aircraft and space probes can be enhanced by image processing algorithms. Most of the image processing techniques developed so far are mainly for enhancing images obtained from unmanned spacecraft, space probes, and military reconnaissance flights.

Face detection problem has been viewed as a two-class classification problem i.e., faces vs. non-face classification problem. There are several techniques developed for face recognition. They are mainly classified as Holistic/template approaches, Feature-based approaches, neural network and Face Recognition. Face Identification generates the final output of the complete face recognition system [2]. It is always important to choose a suitable face classification technique that can provide a good differentiation between different persons..

A. Eigen Faces

In this technique, the Eigen faces method is used for face recognition. Eigenfaces are the word was given to a set of eigenvectors when they are used in the computer vision problem of human face recognition. The eigenfaces themselves form a basis set of all images used to build the covariance matrix. Each image the locations contribute more or less to each eigenvector[3]. So that we can display the eigenvector as a sort if “shadowy” face which we call an eigenface. For the Eigenface algorithm, it falls under two stages. On Specifically, they are the principal components of distribution of faces, or equivalently, the eigenvectors of the covariance matrix of the set of face images, where an image with N x N Pixels is considered a point (or vector) in N2-dimensional space [4][5]. Mathematically, it is simply finding the principal components of the distribution of faces, or the eigenvectors of the covariance matrix of the set of face images, creating an image as a point or a vector in a very high dimensional space[6]. The eigenvectors are ordered, each one accounting for a different amount of the variations among the face images. These eigenvectors can be imagined as a set of features that together characterize the variation between face images. Classification can be achieved by comparing how faces are represented by the basis set. Eigenfaces initialization and eigen faces recognition are the important stages of this algorithm[3][5].

B. Hidden Markov Model (HMM)

Hidden Markov model is designed for face recognition application. In this method scanning mechanism is used to match the face with the existing data base [7]. Scanning mechanism captures two kind of information from the face image. Coordinates of the salient region and local features detected are the two useful information [8]. Scanning is used to calculate the saliency in the face image. Time and storage requirement are the important factors in this analysis. This algorithm takes less storage and shorter time. The main advantage of the hidden Markov models is that the models for each person build independently. So every time we want to add a new person to the collection we just have to add a new model without modifying the other models.

C. Geometric based Algorithm

This is the historical way to recognize people. Geometric

features can be generated by segments, perimeters, and areas of some figures formed by the points. In this algorithm, the facial image is initially analyzed and reduced to a small set of parameters describing prominent facial features such as eyes, nose, mouth and cheekbone curvature. These features are then matched to a database. Results are obtained by comparing the extracted features from the images. Template images are compared with the database images by measuring the distance between them. In FERET protocol, query image is compared with the database images and five closest distance images are brought for final comparison. The approach was robust, but its main problem is the automatic point location. Some problem arises if an image is of bad quality or several points are covered by hair. The major advantage of using this algorithm is that the recognition task is not very expensive. But, the image processing required here is very expensive and parameter selection must be unambiguous to match an individual's face, which becomes a major disadvantage [7].

D. Template Matching Algorithm

Template matching algorithm relies on statistical approach. In this method image pixels are converted into values. Values for different images are stored in database. Query image is converted into value and this value is compared with the database value. Variance is used to predict the closest result. Intensity of the light and orientation of the camera place a major role in this mechanism. For the efficient classification database should consists of multiple images of the same person is required. It only compares the image with the database image. If the image is not in the database it will not give the distant value [7].

E. Face detection algorithm

Face detection algorithm has two major steps. First one is the face localization of the given images in the database. Second one is the feature detection for verifying the face candidates from the localized value. Fig. 1 shows the face detection algorithm. Color image with the pixel sixe 13*13 is given to the system. Lighting compensation technique is used to enhance the image quality. Red, green and blue components are extracted by color space transformation techniques. Skin color is detected using the algorithm. Skin regions are segmented using thresholding method. Skin regions are grouped and the output is generated. In feature detection, Eye and mouth regions are detected using shape localization. With the help of that face boundary is detected and finally the weight values are compared with the database. Face is detected Final Stage.A lighting compensation technique named "reference white" has been introduced to normalize the color appearance. The R,G and B components of the color images are adjusted so that the average gray value of these reference white pixel is linearly scaled to 255.

Fig. 2 shows the basic working principle of the lighting compensation. Here yellow color has been removed. With lighting compensation it detect fewer non-face pixels and more skin tone facial pixels.

F. Face Recognition Using Artificial Neural Networks

Face Detection can be categorized into number of the face recognition system. Classification is based on the ability to focus on the part of an image containing a face. Analysis of facial expression was a simple research field for Physiologists in the past few years such as detection, tracking, recognition, which contributed significantly.ANN techniques were used effectively and in large numbers in the fields of image processing & pattern recognition in Fig. 3.

Face detection involves some steps; they are Feature-based approaches, neural network, and Face recognition. Face Identification generates the final output of the complete face recognition system. It is always important to choose a suitable face classification technique that can provide a good separate ability between different persons.

An image is passed to the system for classification. The image preprocessing is used to remove unwanted noise from lighting and the environment. The classifier used to decide whether the image belongs to the face or non–face class based on information. The output indicates whether the original image contains an image or not. Different Architecture and Modes Used. The modes are as follows [2]:

Rowley, Balviya, and Kanada presented face detection systems based on a retinal connected neural network that examines small windows of an image to decide whether each window contains a face. This system separates many networks to improve performance over other networks. This system used an algorithm called the Bootstrap algorithm as a training process for training the network[9].

Rowley ,Baluja and Kanada explained a neural network based on face detection system. The system consists of multiple networks where the first network is "router" which deals with each input to determine its orientation & then utilize this data to prepare the window.

Jeffrey Noriss used this technique with some linear projection to identify face in real time video streams.System steps to search an image as follows,they are:Select every 20*20 region of input image.Use intensity values of its pixel as 400 input to ANN[10]. If the value is beyond 0.5, the region represents a face.

Loran and Samcovic used ANN for face detection for video surveillance in Fig . 4 . The ANN is trained with multi-layer back propagation network neural network. In this techniques three face representation were taken as Pixel, Partial profile and eigen faces.For these 3 representation ,3 independent sub-detectors are generated. BPNN is used to check if the image include face or not. Gaussian mixture model are fed into BPNN to clarify whether original image includes a face or not.

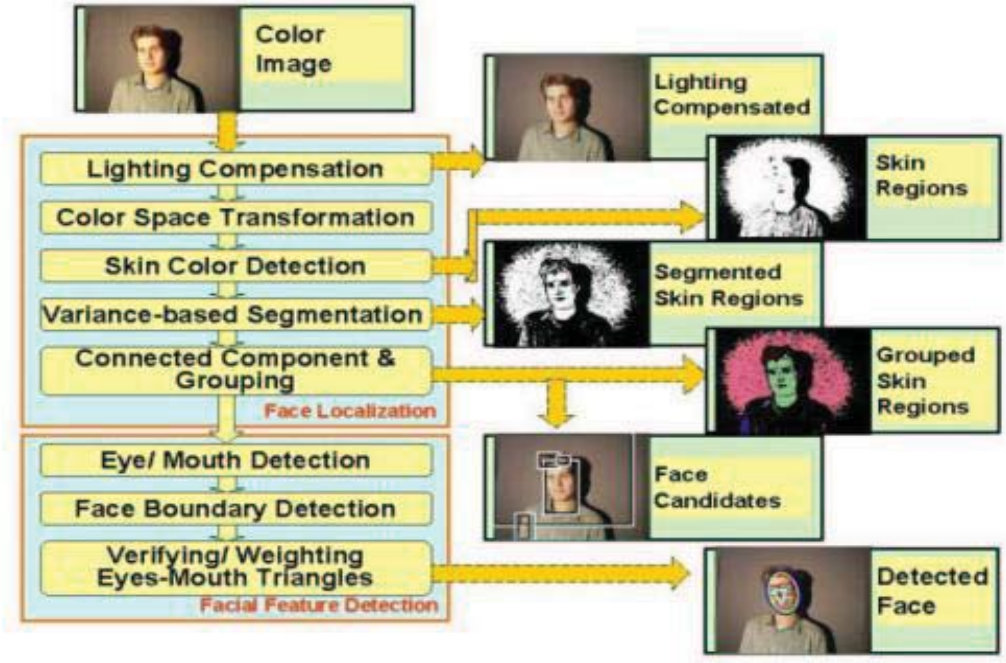

Fig. 1. Face Detection Algorithm

(a) (b) (c) (d)

Fig. 2. Skin detection (a) Yellow biased face image (b) Lightning compensated image
(c) Skin regions of (a) shown in white (d) Skin regions of (b) shown

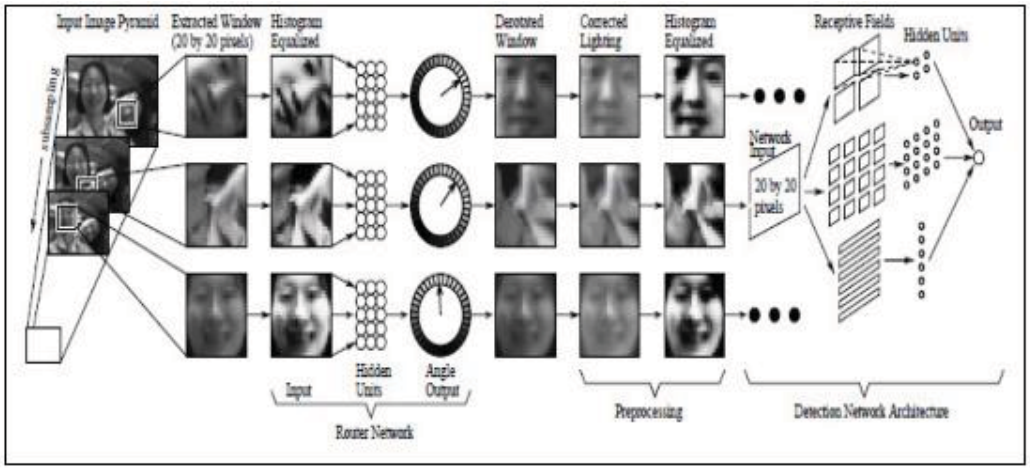

Fig. 3. Rotational Invariant Neural Network for face detection

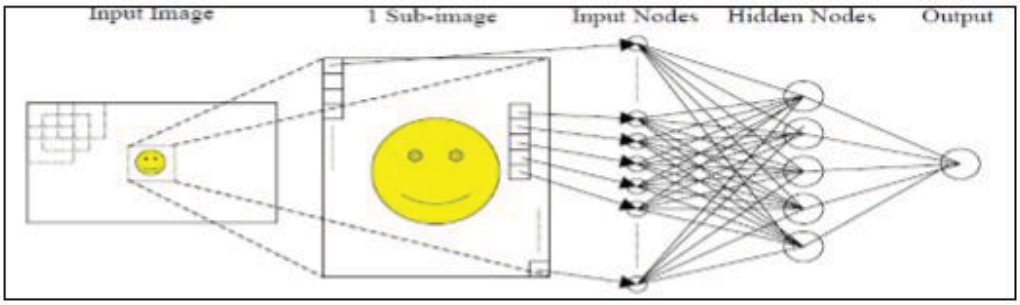

Fig. 4. PCA & ANN for face detection

G. Face Detection using Deep Learning: An Improved Faster RCNN Approach

In modern days, face detection problem is the fundamental problem in images, vision& recognition pattern which was widely known during past few years. In past few years deep learning methods i.e. deep convolutional neural network has achieved or gained success in various computer vision task such as identifying images , classifying images etc. In feature concatenation, for traditional fast RCNN network, ROI pooling is applied to generate features of the region. This approach may sometimes omit some important features. In recent proposed solution, in order to capture more details of ROI, we need to modify the ROI pooling by adding some additional layers. Hard Negative Mining is a strategy or process to boost up the performance of deep learning, especially for object detection task including face detection. This idea behind this method is to detect the network which has failed to make correct prediction. Multi Scale Training is a faster RCNN architecture typically adopt a fixed scale for all training images. By reducing the images to a random scale, the detector will be able to learn features over a wide range of sizes.

III. Conclusion

Here in this work, we have analyzed the different face detection techniques such as eigenfaces, hidden Markov model, geometric based algorithm, template matching algorithm, lighting compensation, and skin tone detection, face recognition using artificial neural networks, principal component analysis with ANN, face recognition using convolutional neural network. In this paper, we surveyed the various face recognition methods and issues faced in real life and how to overcome these issues that can be solved using various image processing techniques and their advantages. To handle issues such as facial aging, pose, occlusion, etc. different techniques are used independently. In order to develop a high performing face recognition system, the integrated approach seems to be a better choice. Now a day's deep learning approach is used to analyze the various feature of a face image.

References

[1] Parveen Kumar, Doulat Singh, "Approach on Face Recognition & Detection Techniques", International Journal of Engineering and Computer Science, ISSN: 2319-7242, Volume 5, Issues 7, July 2016, Page No. 17133-17135.

[2] Omaima N. A. Al-Allaf, "Review of Face Detection Systems Based Artificial Neural Networks Algorithms", The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.1, February 2014, Doi : 10.5121/IJMA.2013.6101.

[3] Kandla Arora," Real Time Application of Face Recognition Concept", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-5, November 2012.

[4] Khashman A., Garad A.A., " Intelligent Face Recognition Using Feature Averaging", In: Mehrotra S., Zeng D.D., Chen H., Thuraisingham B., Wang FY. (eds) Intelligence and Security Informatics. ISI 2006. Lecture Notes in Computer Science, vol 3975. Springer, Berlin, Heidelberg.

[5] C. Suresh Kumar , G.Premalatha , Y. Anusha, "An Approach towards Face Counting System Using Image Processing Techniques", International Journal on Recent Researches In Science, Engineering & Technology, Vol.5, Issue 1,January 2017. ISSN (Print) 2347-6729; ISSN (Online) 2348-3105.

[6] B.S Patil, A.R Yardi," Real Time Face Recognition System Using Eigen Faces", International Journal of Electronics and Communication Engineering & Technology (IJECET), ISSN0976 – 6464(Print), ISSN 0976 – 6472(Online) Volume 4, Issue 2, March – April (2013), © IAEME.

[7] Selvapriya.M, Dr.J.KomalaLakshmi, "Face Recognition Using Image Processing Techniques: A Survey", International Journal Of Engineering and Computer Science ISSN: 2319-7242Volume 3, Issue 12, December 2014, Page No.9704-9711.

[8] Salah, Albert & Bicego, Manuele & Akarun, Lale & Grosso, Enrico & Tistarelli, Massimo. (2007). Hidden Markov Model-based face recognition using selective attention - art. no. 649214. Proceedings of SPIE - The International Society for Optical Engineering. 10.1117/12.707333.

[9] Patrik Kamencay, Miroslav Benco,Tomas Mizdos, Roman Radil, "A New Method for Face Recognition using Convolutional Neural Network", Digital Image Processing and Computer Graphics, volume: 15, Number: 4,2017.

[10] Mrunmayee Vaidya, Jigyasa Solanki,Sravani Wayangankar "Face recognition using CNN", International Journal of Advance Research, Ideas and Innovations in Technology, Volume 5, Issue 3.