IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 07 (July. 2014), ||V2|| PP 49-54

Facial Recognition System: A Review

Ankita[1], Dr. Sanjay Kumar Malik[2]
[1]*M. Tech Scholar, Hindu College of Engineering*
[2]*Assistant Professor, Hindu College of Engineering*

Abstract: - Face is the mirror of human emotions, characteristics and the behavior. This is proved by the biometric science. A lot of work has been earlier carried out with face and facial features. Such biometric systems are used for application authentication as well as for web authentication. Apart from that they are used to identify the criminals, age, gender on the basis of facial features. The accuracy of these systems depends on the facial features. It also depends on how they are detected and what kind of information can be retrieved from the face. The proposed work is in the same direction to identify different kinds of features that can be identified from the face. Our work includes all the physical, behavioral and functional features of the face. This paper has made a comparison between different facial feature detection methods. The comparisons will be taken in terms of number of features detected, time taken to detect the feature and the accuracy of the extracted features.

Keywords: *Face Recognition, Behavioral Challenges, Biometric System, Facial Biometric System.*

INTRODUCTION

Face is the most visible part of a human which enables to identify a person uniquely. A face conveys all kinds of information regarding a person, including the individual nature, behavior, age, gender, emotion, expression etc. While working with biometric science
face is the first target to perform the biometric processing. It is always tried to build a system that can perform the decision making recognizing the face, like
a human being does in his social life. While working with facial biometric processing there are number of operations being performed such as Face Detection, Recognition, Tracking, Modeling of Face, its analysis etc. The Facial Biometric does not mean the face only. It also includes different human parts individually that can help to perform all kinds of decision making individually. These organs include the Human Eyes, Eye Gazes, Eye Movement, Lips and Ear etc. Each itself can perform a complete decision making individually.

In this presented work, we are performing an analysis for different Facial biometrics including the Face, Eyes and Lips. We have highlighted the difference in facial features respective to Age, Emotions, Expressions and Gender. The feature extraction is performed using different extraction methods like Gabor Filter, Morphological operators, Markov Model, Fisher Algorithm etc. Here we are presenting a comparative study on all these methods respective to the facial features.

HISTORY

The concept of Face, Facial Expression and Facial Recognition is too old than the invention of computer system. Even in social life, the first and foremost identification of a person is his face. All kinds of social decisions are based on the person's face identification. That is the only reason with begin of computer vision the work in same area begin. The dire need of such system was realized when most of the password based authentication system encountered number of flaws. The software made for authentication was cracked by some intelligent software or the person. So, there was the requirement to attach the person itself with computer system which gives rise to the invention of biometric system. The biometric not only include the face but it also includes the finger, thumb, vein, voice, signature, eyes etc. Each biometric feature has its own advantages and disadvantages.

A biometric system has the following features

- A Biometric feature or object is differentiated in terms of availability. It means either the object is available online or offline. In case of offline the work is done on the images whereas in case of online system the work is performed by including some device with the system. These devices extract the biometric information and pass it to the biometric system which will impart some output on the basis of which the concerned decision will be taken place.
- User interference is another feature of a Biometric object that defines the use of the biometric feature. There are some biometric objects that can be modified by the individual whereas some cannot be changed in any way. Such as Signature are completely copied or changed by any individual. Eyes can be inferred by using contact lenses, glasses etc. Face can be modified with Beard, makeup etc.

- Some biometric objects are influenced by the surroundings also such as voice. A voice system also includes some noise. A facial recognition system can also be affected with the background, lighting effect etc.

Instead of all these complications and the features, each biometric feature must be recognized uniquely. To perform this identification or the recognition we need a separate system for each object. It means the similar Biometric system cannot be used for every object. Each biometric system follows a common biometric model represented in figure 1

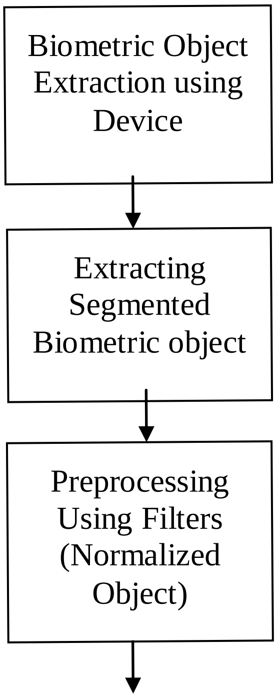
Each Biometric system itself contains a source dataset in the form of biometric images. These images are maintained in a database in the normalized form. As soon as a person enters into the system, biometric image extraction is performed for identification of facial features. The extraction process is done using some biometric device such as in case of face it can be a Web Cam or the video. As the biometric image is extracted it still contains some noise such as the wider object area. Some segmentation is performed on this biometric object to get the exact object area. On this extracted object image some filtration is performed to convert the main object to the normalized object. The normalization is the actual featured object on which all kind of decision making can be performed. Finally from these objects different kind of features are extracted. By using these features, object is compared with database objects and the final decision making is performed which leads to acceptance or the rejection of the object.

Although the model is same for all kind of biometric system but these systems or the biometric objects vary in different ways. There is an identical biometric system for each biometric object. It means the biometric system for one object will not work for other as each object has a unique extraction process, unique filtration sequence and a separate set of functional, physical and behavioral characteristics.

I. FACIAL BIOMETRIC SYSTEM

Here, we are working with Face and Facial Biometric System. Facial biometric processing is one tool in the same direction. The survey on the face recognition is made in 1995 by R. Chellappa. But the analysis was started on the face in late 90's. A major work had been done till the end of 1990 on the face and the facial features. In earlier stages the faces are detected on the basis of distance analysis or its alignment position or the autocorrelation matrices. After that this work is forwarded with different technologies. A face biometric system has a lot of advantages and disadvantages.

1. A facial system can be online or the offline system. It means we can perform the facial processing either from the image or we can extract the image from online means such as the Webcam. Such kind of system can be attached along with a web application that will accept the human face from webcam as the password to the system.
2. A face can represent the human expressions and emotions clearly such as anger, cry, laugh. For each emotion the system will return an individual face image. We use facial system in such application


Biometric Object Extraction using Device
Extracting Segmented Biometric object
Preprocessing Using Filters (Normalized Object)

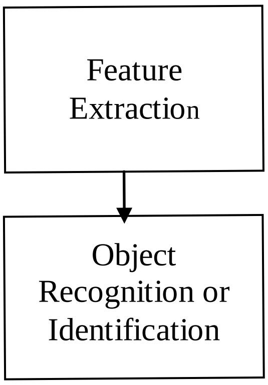


Fig. 1: Biometric System

where expression plays an important role such as in medical science the facial expressions are used to identify the pain.

3. The face is the most visible feature of a human. It helps a user to identify any mistake of the computer based recognition system as the results can be verified by the user, i.e. the results given by pain recognition system can be verified by the doctor by observing the patient’s face.
4. Facial Biometric system has different applications according to the facial features. It can be used as an identification system for any application or any website. It can also be used as criminal identification system.

II. LITERATURE SURVEY

The ancient Egyptians and the Chinese played a vital role in biometrics' history. Although biometric technology belongs to the twenty-first century, the history of biometrics goes back thousands years. Today, the focus is on using biometric recognition and identifying characteristics to improve security measures. Once an individual is matched against a template, or sample, in the database, a security alert goes out to the authorities. Biometric technologies also need to achieve greater standardization and technological innovations to be recognized as a trustworthy identity authentication solution. European recorded the first known example of fingerprinting, which is a form of biometrics, in China during the 14th century. Chinese merchants used ink to take children's fingerprints for identification purposes. In 1890, a Parisian police desk studied body mechanics and measurements to help in identification of criminals. In the 1960s and '70s, signature biometric authentication procedure was developed, but the biometric field remained fixed to the military and security agencies research which developed biometric technology beyond fingerprinting.

Biometrics is a growing and controversial field in which civil liberties groups express concern over privacy and identity issues. Today, biometric laws and regulations are in process and biometric industry standards are being tested. Face recognition biometrics has not only reached the prevalent level of fingerprinting, but the constant technological pushes and with the threat of terrorism, researchers and biometric developers will hone the security technology for the twenty-first century.

Anil K. Jain, Arun Ross and Salil Prabhakar [1] designed a Biometric Recognition system using the four main modules:

1. *Sensor module*, which captures the biometric data of an individual.
2. *Feature extraction module*, in which the acquired biometric data is processed to extract a set of salient or discriminatory features.
3. *Matcher module*, in which the features during recognition are compared against the stored templates to generate matching scores.
4. *System database module*, which is used store the biometric templates of the enrolled users.

Weicheng Shen and Tieniu Tan [2] have proposed a typical automated biometrics-based identification/verification system that consists of the following major components:

1. *Data acquisition component* acquires the biometric data in digital format by using a sensor.
2. *Feature extraction component* uses an algorithm to produce a feature vector in which the components are numerical characterizations of the underlying biometrics. The feature vectors are designed to characterize the biometrics so that biometric data can be collected from an individual, at different times that are ‘‘similar,’’ while those collected from different individuals are ‘‘dissimilar.’’ In general, the larger the size of a feature vector (without much redundancy), the higher will be its discrimination power which is defined as the difference between a pair of feature vectors representing two different individuals.

3. *Matcher component* compares feature vectors obtained from the feature extraction algorithm to produce a similarity score. This score indicates the degree of similarity between a pair of biometrics data under consideration.
4. *Decision-maker component* is the last component of the system that finally provides/rejects access to the user based on some pre-determined criterion.

Arun Ross, Anil Jain [3] proposed Multibiometric system which seeks to alleviate some of the drawbacks of single biometric system by providing multiple evidences of the same identity. These systems help to achieve an increase in performance that may not be possible by using a single biometric indicator. Multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. The authors proposed Fusion in biometrics with certain levels.

Madalin Tefan Vlad, Razvan Tatoiu, Valentin Sgarciu [4] proposed an integrated system for automatic identification, using smart card and fingerprint features. The goal is to do both a biometric identification as well as verification, with the personal data stored on the smart card. The first important step is considered to be the enrollment. Therefore, a new user, who will be involved in the system, comes to an authority and gets his finger scanned for several times (usually 3-5 times), in order to get the best fingerprint. From the images captured by the biometric sensor, the features are extracted, and the best feature string, with maximum number of minutiae will be stored on the smart card. Sending and storing the minutiae string on the smart card are done in a secure way, with several mechanism of authentication, in order to perfectly protect the personal data.

To understand the concept of facial intension identification we need to understand the facial recognition, Eyes Recognition etc. The concept of face recognition is too old. In 1967 a machine learning face recognition system was presented in which an image is projected to a photomultiplier matrix and a weighted value is assigned to cells of matrices on the basis of which decision making is performed. An image is presented about 250 times on this matrix and after this each image gives 100% accurate results [11]. In 1976, a pattern recognition system was proposed to identify the face. This approach gives an algorithm to pattern recognition by dividing the whole process in 4 stages i.e. Image acquisition, Preprocessing, Feature Extraction and the Discrimination. The system worked with black and white images taken from television cameras only. They required all images to be in proper format in terms of size, lighting, threshold values etc which gives the accuracy up to 90%. [12].

In 1989 a work was performed where the images were compared on the basis of extracted part not on whole image. In this approach at first the surface of the face image is extracted. This extracted surface is presented in the form of a curvature. Once the curvature is extracted then this part of image is used for the image identification. The image comparison is basically performed on the basis of quadratic distance between the source image and the database image [13]. As the comparison results were based on threshold values the results were not so realistic. A neural network based approach for face identification was presented by M. A. Kerin in 1990. This approach partitioned the faces in disjoint classes respective to the attributes. Instead of working on whole dataset, the work was performed in the form of clusters which gave it a new significant level of the result accuracy.[13]. In 1991, a PCA (Principal Component Analysis) based approach was used to identify the face images. This approach was based on the concept of Eigen Faces and Eigen vector. For the m number of images n Eigen vectors are drawn. Database images are trained by using PCA approach and in the same way the source images also give the respective Eigen vector. Once Eigen vector is extracted then this Eigen vector is compared with Eigen vectors of database images and the image with lowest Euclidean distance will be selected as the identified image. PCA is basically a vision based approach to identify the images which compress the data and generate a vector on which the decision making is performed [14]. The Eigen value approach becomes the baseline for most of the other images.

In the same year 1991, a location based approach was implemented to identify the face for the authentication system. This approach performs the comparison using main facial features like chin, eyes, nose, head etc. The work is tested on about 397 face images and a good outcome of 90% accuracy is identified. But the system does not work for the unknown faces. This approach represents the identification rate for feature of each face separately [15]. This approach worked only for faces with rage movement after that the approach started giving the worst results.

III. CHALLENGES

Ageing: - One of the major problem in face recognition is the change in facial features because of ageing. Facial ageing is the complex process that includes the change in term of complexion, shape, wrinkles etc. Ageing is not only the problem for face recognition process but there also exist number of applications that are correlated to ageing concepts [1] such as Recognition of missing persons based on his older image, detection of multiple enrollments or multiple accounts of a person, Age estimation etc. The key point of ageing is the growth factor analysis as well as the properties that will be changed along with the growth such as texture, skin tone etc. The approach which gives the recognition independent to person’s age is called non-generative approach [2].

Image Quality: - Image Quality is another important factor that depends on the database images and the input image quality. The quality of image can differ because of the device used for image extraction. Some other factors that influence the image quality are the difference in image resolution, illumination, contrast distortion, loss of correlation etc.[3]. Most of the problems in image quality are because of the tool or the device used for the image extraction. To get the invariance in terms of image quality it is required to analyze the image quality and match them respectively with external features. There are number of approaches which are used to perform the image quality analysis using some quantitative methods. These methods include the Image Intensity difference analysis. This measure is used to compare the magnitude of two images based on intensity level. The other measure is the analysis of image irregularity. For this, edge based approach is used to perform the analysis. To analyze the image data error the MSE(Mean Square Error) or PSNR(Peak signal to noise ratio) can be used[4].

Face Expressions:- Face Expressions include diversion of the frontal face image in the training image, and the testing image is another major criterion that increases the complexity in face recognition. To build an application based on expression invariant one requires to perform an intuitive analysis in the recognition process effectively. As the expression changes, the structure of face changes in terms of displacement of features, change in distance between eyes, and change in shape of lips etc. To get the effective analysis geometrical comparison is required to be performed. To get the robustness based on this feature generally a series of images are trained [5].

IV. APPLICATIONS

Face recognition has the great impact in the industry because of its versatile applications. The recognition process is best utilized to identify the missing persons or the criminals. In most of the industrial applications, where the security is major criteria, the traditional password based authentication system is replaced by facial identification system. There are number of realtime and the simulation based application in which the face recognition is being used extensively. The major concern of the face recognition is the security which includes the identification and the verification task[6]. In such kind of identification process, the robustness is required in terms of ageing and the face expressions. It also requires identifying the face images based on half face comparison or the structural analysis because in such application the test image can differ in terms of some major changes in face image.

V. DATA COLLECTION

As we can understand, in Facial Biometric system the reliability depends on the dataset on which the algorithm or the system is tested. It means to find the better reliability in terms of derived results we require a larger database that can have different kinds of face images. The database must include :

a. Dataset having images of both males and females.
b. Dataset should have images of different age groups.
c. Dataset having the images with different facial emotions and the expressions.
d. Dataset having the different picture quality.
e. Dataset of different file formats.
f. Dataset of different face positions.
g. Dataset should contain number of instances of a person’s image.

VI. CONCLUSION

In this paper, a detailed exploration to the face detection and facial feature detection is performed. The paper has presented the standard model for facial feature detection and recognition along with the exploration of associated applications and challenges.

REFERENCES

[1] Anil K. Jain, Arun Ross and SalilPrabhakar2, “*An Introduction to Biomertics Recognition*”, IEEE Transactions on Circuits and Systems for Video Technology, Special issue on Image-and-Video-Based Biomertics, Vol 14, No. 1, January 2004

[2] Weicheng Shen and Tieniu Tan, “*Automated Biomertics-based personal Identification*”, Arnold and Mabel Beckman Center of the National Academics of Sciences and Engineering in Irvine,CA, August 1998

[3] Arun Ross, Anil Jain, "*Information Fusion in Biomertics*", Department of Computer Science and Engineering, 2002

[4] Madalin Tefan Vlad, Razvan Tatoiu, Valentin Sgarciu, "*Smart Card and Biometrics used for Secured Personal Identification System Development*", Automatic Control and Computers Department, University Politehnica of Bucharest, 2000

[5] Dr. Tang, Yuan Yan, Dr Leung and Yin Wing, "*Fingerprint Recognition*", Department of Computer Science and Engineering, April 2002

[6] Jun Ou，Xiao-Bo Bai, "*Automatic Facial Expression Recognition Using Gabor Filter And Expression Analysis*", Second International Conference on Computer Modeling and Simulation 978-0-7695-3941-6/10© 2010 IEEE

[7] Caixia Yang, Jiande Sun, Ju Liu, "*A Gray Difference-Based Pre-Processing for Gaze Tracking*", 978-1-4244-5900-1/10©2010 IEEE

[8] Zhiwei Zhu and Qiang, "*Novel Eye Gaze Tracking Techniques Under Natural Head Movement*", 0018-9294 © 2007 IEEE

[9] Liu Tao Pang Changle, "*Eye-gaze Tracking Research Based on Image Processing*", 2008 Congress on Image and Signal Processing 978-0-7695-3119-9/08 © 2008 IEEE

[10] Xue Yuan, Jianming Lu and Takashi Yahagi, "*Biometrics Verification Using Palm Vein- Patterns*", Chiba University, 1-33, Yayoi-cho, Inage-ku, Chiba, Japan, 2002

[11] Sang Kyun, Hwan Soo Choi, and Soo-Won Kim, "*A Direction-based Vascular Pattern Extraction Algorithm for Hand Vascular Pattern Verification*", ETRI Journal, Vol 25, No. 2, April 2003

[12] Sang Kyun, Hyung-Man Park, Young-Woo Kim, Sang-Chan Han, Soo-Won Kim and Chul-Hee Kang, "*A Biometric Identification System by Extracting Hand Vein Patterns*", Department of Electronics Engineering at Korea University, Journal of Korean Physical Society, Vol 38, No.3, March 2001