FACE RECOGNITION TECHNIQUE

Karshnik Singh [1], Navneet Vishnoi[2]
[1]*MCA(LE)4th sem, CCSIT, TMU ,Moradabad*
[2]Assistant Professor, CCSIT, TMU, Moradabad
[1]*karshniksingh@gmail.com*
[2] navneetvishnoi@gmail.com

***Abstract: Over* the last ten years or so, facial recognition has become a popular area of research in computer vision and one of the most successful applications of image analysis and understanding. Because of the nature of the problem, not only computer science researchers are interested in it, but neuroscientists and psychologists also. It is the general opinion that advances in computer vision research will provide useful insights to neuroscientists and psychologists into how human brain works, and vice versa. Humans have always had the innate ability to recognize and distinguish between faces, yet computers only recently have shown the same ability. In the mid 1960s, scientists began work on using the computer to recognize human faces. Since then, facial recognition software has come a long way. In this article, we will look at the reason behind using facial recognition, the various technology used in the facial recognition, the products been made to implement this biometrics technique and also the criticisms and advantages that are bounded with it**.

I. INTRODUCTION

Biometric recognition, or biometrics, refers to the automatic identification of a person based on his/her anatomical (e.g., fingerprint, iris) or behavioral (e.g., signature) characteristics or traits. This method of identification offers several advantages over traditional methods involving ID cards (tokens) or PIN numbers (passwords) for various reasons: (i) the person to be identified is required to be physically present at the point-of-identification; (ii) identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased integration of computers and Internet into our everyday lives, it is necessary to protect sensitive and personal data. By replacing PINs (or using biometrics in addition to PINs), biometric techniques can potentially prevent unauthorized access to ATMs, cellular phones, laptops, and computer networks. A biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific anatomical or behavioral characteristic possessed by the user. Examples: Healthrow airport, pay by touch, smart gate, iris based ATM, time and attendance.

II. CLASSIFICATION OF BIOMETRICS

1. Fingerprint SDKs- A fingerprint SDK is a software toolkit that allows software developers to integrate a fingerprint recognition system into a variety of applications. Fingerprint SDKs provide a low-level framework to communicate with the fingerprint reader, capture an image, extract the unique minutiae data from the image, and compare two sets of extracted minutiae data.

2. Face SDKs- Face SDK is a high-performance, multi-platform face identification and facial feature recognition solution. Serving software developers worldwide, Face SDK is a perfect way to empower Web and desktop applications with face-based user authentication, automatic face recognition, and identification.

3. Eye Iris SDKs- Eye iris identification technology is intended for biometric systems developers and integrators. Eye iris is available as a software development kit that allows development of PC- and Web-based solutions on Microsoft Windows, Linux and Mac OS X platforms.

4. Voice SDKs- voice identification technology is designed for biometric systems developers and integrators. The text-dependent speaker recognition algorithm assures system security by checking both voice and phrase authenticity. Voiceprint templates can be matched in 1-to-1 (verification) and 1-to-many (identification) modes.

➢ Facial Recognition

A facial recognition 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 to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

➢ Why Face Recognition?

Currently there are many methods of biometric identification and each of these methods has certain advantages and disadvantages which must be considered in developing biometric systems, such as: system reliability, price, flexibility, necessity of physical contact with the scanning device and many others. Selecting a certain biometric identification method or using a multibiometric system can help to support these often discrepant requirements. Face recognition can be an important alternative for selecting and developing an optimal biometric system. Its advantage is that it does not require physical contact with an image capture device (camera). A face identification system does not require any advanced hardware, as it can be used with existing image capture devices (webcams, security cameras etc.). Thus, facial recognition should be considered as a serious alternative in the development of biometric or multi-biometric systems.

➢ Basic Recommendations for Facial Recognition

Face recognition accuracy heavily depends on the quality of a face image. There are some basic recommendations and constraints when using face recognition applications.

1) Cameras and images

 Similar quality cameras are recommended for both enrollment and identification. Using the same camera model is even better.
 50 pixels is the recommended minimal distance between eyes for a face on image or video stream to perform face template extraction.
 75 pixels or more recommended for better face recognition results. Note that this distance should be native, not achieved by resizing an image.
 Lower resolution webcams are not recommended as optical distortions will appear and affect facial template quality because users will have to be too close to the cameras for successful face detection and enrollment.

2) Lighting

Controlled lighting conditions are recommended:

 Direct frontal or diffused light allows equal lighting distribution on each side of the face and from top to bottom with no significant shadows within the face region.
 Avoid glares on face skin or glasses that are produced by some types of illumination.

3) Facial expression

Neutral face expression during enrollment is recommended, as non-neutral face expression may affect the accuracy of recognition. Examples of non-neutral face expressions (they are allowed but not recommended):

 Broad smile (when teeth or the inside of the mouth exposed).
 Raised eyebrows.
 Closedeyes.
 Eyes looking away from the camera.

Slight changes in facial expression are acceptable during identification, as they do not influence the accuracy of face recognition.

4) Glasses, Makeup, Hair, Beard and Moustache

Several images with different appearance variants are recommended for assuring the quality of recognition in the situations when part of face is covered with glasses or hair:

 Eyeglasses– separate enrollments with and without glasses will assure the best recognition quality for both cases. Special recommendations:
 Sunglasses and regular glasses with heavy frames will decrease recognition quality, as they cover part of face and some facial features become not visible. If possible, they should be avoided during both enrollment and identification.
 Contact lens– the contact lens do not affect the recognition quality. However, persons wearing them sometimes may wear eyeglasses instead of lens. In this case an additional enrollment with eyeglasses is recommended.
 Heavy makeupis not recommended as it can hide or distort facial features.
 Hair style– some hair styles may cover parts of face, thus hairpins or other means of holding hair off the face are recommended during enrollment.
 Facial hair style changes may require additional enrollments, especially when beard or moustache is grown or shaved off.

➢ Finding Faces in Images

Given an image, which can come from a file or from live video, the face detector examines each image location and classifies it as "Face" or "Not Face." Classification assumes a fixed scale for the face, say 50x50 pixels. Since faces in an image might be smaller or larger than this, the classifier runs over the image several times, to search for

faces across a range of scales. This may seem an enormous amount of processing, but thanks to algorithmic tricks, explained in the sidebar, classification is very fast, even when it's applied at several scales. The classifier uses data stored in an XML file to decide how to classify each image location. The OpenCV download includes four flavors of XML data for frontal face detection, and one for profile faces. It also includes three non-face XML files - one for full body (pedestrian) detection, one for upper body, and one for lower body.

III. FACIAL RECOGNITION TECHNOLOGY

Like fingerprint biometrics, facial recognition technology is widely used various systems, including physical access control and computer user accounts security. Usually these systems extract certain features from face images and then perform face matching using these features. A face does not have as many uniquely measurable features as fingerprints and irises, so facial recognition reliability is slightly lower than these other biometric recognition methods. However, it is still suitable for many applications, especially when taking into account its convenience for user. Facial recognition can also be used together with fingerprint recognition or another biometric method for developing more securitycritical applications. The multi-biometric approach is especially important for identification (1-to-many) systems. In general, identification systems are very convenient to use because they do not require any additional security information (smart cards, passwords etc.). However, using 1-to-many matching routines with only one biometric method can result in a higher false acceptance probability, which may become unacceptable for applications with large databases. Using face identification as an additional biometric method can dramatically decrease this effect. This multi-biometric approach also helps in situations where a certain biometric feature is not optimal for certain groups of users. For example, people who do heavy labor with their hands may have rough fingerprints, which can increase the false rejection rate if fingerprint identification was used alone. Some facial recognition algorithms identify faces 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 detection. A probe image is then compared with the face data. Recognition algorithms can be divided into two main approaches, geometric, which look 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.

➢ 3-dimensional recognition

A newly emerging trend, claimed to achieve improved accuracies is three-dimensional face recognition. This technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin. One advantage of 3D facial recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view. Three-dimensional data points from a face vastly improve the precision of facial recognition.

➢ Skin texture analysis

Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person’s skin into a mathematical space. Tests have shown that with the addition of skin texture analysis, performance in recognizing faces can increase 20 to 25 percent.

➢ Software

 Google's Picasa digital image organizer has a built in face recognition system starting from

version 3.5 onwards. It can associate faces with persons, so that queries can be run on pictures to return all pictures with a specific group of people together. Picasaweb.com has also been providing a similar feature to its users.

- Apple iPhoto, photo organizer distributed with iLife suite of applications includes a system by which people can tag recognized people on photos. Then they can be searched using Spotlight.
- Sony's Picture Motion Browser (PMB) analyses photo, associates photos with identical faces so that they can be tagged accordingly, and differentiates between photos with one person, many persons and nobody.
- Facebook also included face recognition technology
- Windows Live Photo Gallery also included face recognition in last version.

IV. RELATED PRODUCTS OF FACIAL RECOGNITION

VeriLook SDK-

The VeriLook technology is intended for facial recognition system integrators. VeriLook offers fast, reliable identification with live face detection and the ability of multiple face processing in a single frame. VeriLook 5.2 SDK is camera independent, webcam capable and offers a set of programming samples and tutorials written in major programming languages. These types of SDK are available:

- VeriLook 5.2 Standard SDK is intended for PCbased biometric application development. It includes Face Matcher and Face Extractor components, programming samples and tutorials, fingerprint scanner support modules and software documentation. The SDK allows the development of biometric applications for Microsoft Windows, Linux or Mac OS X operating systems.
- VeriLook 5.2 Extended SDK is intended for biometric Web-based and network application development. It includes all features and components of Standard SDK. Additionally, the SDK contains Face Client component and a ready-to-use matching server.

VeriLook Embedded SDK-

VeriLook Embedded facial identification technology is intended for mobile biometric systems developers and integrators. The technology assures simultaneous multiple face recognition and face matching in 1-to-1 and 1-to-many modes with PC-like reliability. VeriLook Embedded is available as a software development kit that allows
has been the basis for several other face recognition based security systems, where the technology itself does not work particularly well but the user's perception of the technology does.

3. Privacy Issues Many citizens express development of stand-alone or Web-based solutions for Smartphone's, tablets and other devices that are running Android OS.

VeriLook Surveillance SDK

VeriLook Surveillance SDK is intended for developing biometric software that performs face identification using live video streams from high-resolution digital surveillance cameras. The technology is suitable for passive biometric identification – when passers-by do not make any efforts to be recognized. List of possible uses includes law enforcement, security, attendance control, visitor counting and other commercial applications.

The VeriLook Surveillance SDK includes support modules for a list of high-resolution digital cameras as well as supports regular webcams. The SDK allows creating applications for Microsoft Windows and Linux platforms.

MegaMatcher SDK-

MegaMatcher is a multi-biometric technology, intended for large-scale AFIS or multi-biometric face, fingerprint, iris and palm print system integrators. The technology includes face, fingerprint, iris and palm print recognition engines that could be used either separately or together. MegaMatcher 4.3 SDK includes server software for local multi-biometric systems, cluster software for

largescale multi-biometric products development, and a set of valuable task-specific components.
MegaMatcher on Card Software Development Kit (SDK)-

MegaMatcher on Card is based on MegaMatcher multi-biometric AFIS technology and intended for systems that match faces, fingerprints and/or irises on smart card. MegaMatcher On Card 3.1 SDK includes smart cards with pre-loaded face, fingerprint and iris matching engines, as well as PC-side face, fingerprint and iris template extraction components.

V. CRITICISMS OF FACIAL RECOGNITION

1. Weaknesses

Face recognition is not perfect and struggles to perform under certain conditions. Ralph Gross, a researcher at the Carnegie Mellon Robotics Institute, describes one obstacle related to the viewing angle of the face: "Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there've been problems." Other conditions where face recognition does not work well include poor lighting, sunglasses, long hair, or other object partially covering the subjects face, and low resolution images. Another serious disadvantage is that many systems are less effective if facial expressions vary. Even a big smile can render the system less effective. For instance: Canada now allows only neutral facial expressions in passport photos.

2. Effectiveness

Critics of the technology complain that the London Borough of Newham scheme has, as of 2004, never recognized a single criminal, despite several criminals in the system's database living in the Borough and the system having been running for several years. "Not once, as far as the police know, has Newham's automatic facial recognition system spotted a live target."This information seems to conflict with claims that the system was credited with a 34% reduction in crime (hence why it was rolled out to Birmingham also).However it can be explained by the notion that when the public is regularly told that they are under constant video surveillance with advanced face recognition technology, this fear alone can reduce the crime rate, whether the face recognition system technically works or does not. Thisconcern that their privacy is being compromised by the use of surveillance technologies by corporations and the state. Some fear that it could lead to a "total surveillance society," with the government and other authorities having the ability to know the whereabouts and activities of all citizens around the clock. This knowledge has, is and could continue to be deployed to prevent the lawful exercise of rights of citizens to criticize those in office, specific government policies or corporate practices. Many centralized power structures with such surveillance capabilities have abused their privileged access to maintain control of the political and economic apparatus and curtail populist reforms. Facial recognition can be used not just to identify an individual, but also to unearth other personal data associated with an individual – such as other photos featuring the individual, blog posts, social networking profiles, Internet behavior, travel patterns, etc. – all through facial features alone.[19] Moreover, individuals have limited ability to avoid or thwart facial recognition tracking unless they hide their faces. This fundamentally changes the dynamic of day-to-day privacy by enabling any marketer, government agency, or random stranger to secretly collect the identities and associated personal information of any individual captured by the facial recognition system.

VI. BENEFITS OF BIOMETRIC FACIAL SYSTEMS

- *No More Time Fraud* - One of the big benefits of using face biometric systems in your company is that you won't have to worry about time fraud. It will be impossible for buddy punching to occur, since everyone has to have their face scanned to clock in.
- *Better Security* - You'll also enjoy better security with a facial biometrics system. Not only can you

track employees, but any visitors can be added to the system and tracked throughout the area too. Anyone that is not in the system will not be given access.

 Automated System - Many companies like the fact that biometric imaging systems are automated. You won't have to worry about having someone there to monitor the system.

 Easy Integration - Biometric facial systems are also easy to integrate into your company. Usually they will work with existing software that you have in place.

 High Success Rate - Facial biometrics technology today has a high success rate, especially with the emergence of 3d face recognition. It is extremely difficult to fool the system, so you can feel secure knowing that your system will be successful at tracking time and attendance while providing better security.

VII. CONCLUSION

We have so far able to understand the meaning of biometrics, its different types in brief. Also we have studied the facial recognition meaning and techniques. In the end of this paper, we will be able to acquire a good knowledge about the facial recognition.

VIII. ACKNOWLEDGEMENT

This research was supported/partially supported CCSIT, Teerthanker Mahaveer University, Moradabad. I take this opportunity to express my immense gratitude to my project guide **Mr. Navneet Vishnoi** in my research on Face Recorgnaization. I am grateful for their prolonged interest in my work and excellent guidance. They have been a constant source of motivation to me. I am highly beholden to **PRO. R. K. Dwivedi**, Principal of ―College of Computing Sciences And Information Technology" for his valuable direction and timely idea in my research.

REFERENCES

1) Face Recognition: a Summary of 1995 – 1997 by Thomas Fromherz
2) Face recognition: eigenface, elastic matching and neural nets Jun Zhang;Yong Yan; Lades, M. Proceedings of the IEEE Volume 85, Issue 9, Sep 1997 Page(s):1423 – 1435
3) Thomas Fromherz, Peter Stucki, Martin Bichsel "A Survey of Face Recognition", MML Technical Report, No 97.01, Dept. of Computer Science, University of Zurich.
4) Y.L.Tian and R. Bolle. Automatic detecting neutral face for face authentication. In Proceedings of AAAI03 Spring Symposium on Intelligent Multimedia Knowledge Management, CA, 2003.
5) Comprehensive Database for Facial Expression Analysis BY Takeo Kanade Jeffrey F. Cohn, Yingli Tian
6) V. Blanz and T. Vetter. A morphable model for the synthesis of 3d faces. In Computer Graphics Proceedings, Annual Conference Series (SIGGRAPH)
7) Wlodzimierz M. Baranski, Andrzej WytyczakPartyka, Tomasz Walkowiak, "Computational complexity reduction in PCA based face recognition", Institute of Computer Engineering, Control and Robotics, Wroclaw University of Technology, Poland.