ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Facial Recognition Technology

Prof. Alaka Khemnar [1], Prof. Mayuri Dangare [2] , Prof. Nilima Dhokane[3] , Kishansinh Rathod [4]

Assistant Professor, Department of Computer Science, Sinhgad College of Science, Ambegaon Pune, Maharashtra, India [1,2,3],

Student of M.Sc (Computer Science), Sinhgad College of Science, Ambegaon, Pune, Maharashtra, India [4]

ABSTRACT: A face recognition technology is used to automatically identify a person through a digital image. It is mainly used in security systems. The face recognition will directly capture information about the shapes of faces. The main advantage of facial recognition is it identifies each individual's skin tone of a human face's surface, like the curves of the eye hole, nose, and chin, etc. this technology may also be used in very dark condition. It can view the face in different angles to identify.

KEYWORDS: Biometric, illumination, face print

I. INTRODUCTION

Face Recognition is one of the key areas under research. It has number of applications and uses. Many methods and algorithms are put forward like, 3D facial recognition etc. Face recognition comes under Biometric identification like iris, retina, finger prints etc. The features of the face are called biometric identifiers. The biometric identifiers are not easily forged, misplaced or shared hence access through biometric identifier gives us a better secure way to provide service and security. We can also develop many intelligent applications which may provide security and identity these systems can be well incorporated into mobile and embedded systems efficiently and can be utilized on larger scale. Face recognition becomes challenging with varied illumination and pose conditions. This method over comes the varied illumination problem and detection in noisy environments.

II. WHAT IS FACIAL RECOGNITION TECHNOLOGY

Facial recognition analyzes the characteristics of a person's face images input through a digital video camera. It measures the overall facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are retained in a database and used as a comparison when a user stands before the camera. This biometric has been widely, and perhaps wildly, touted as a fantastic system for recognizing potential threats (whether terrorist, scam artist, or known criminal) but so far has not seen wide acceptance in high-level usage. It is projected that biometric facial recognition technology will soon overtake fingerprint biometrics as the most popular form of user authentication.

Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. Each human face has approximately 80 nodal points. Some of these measured by the Facial Recognition Technology are:

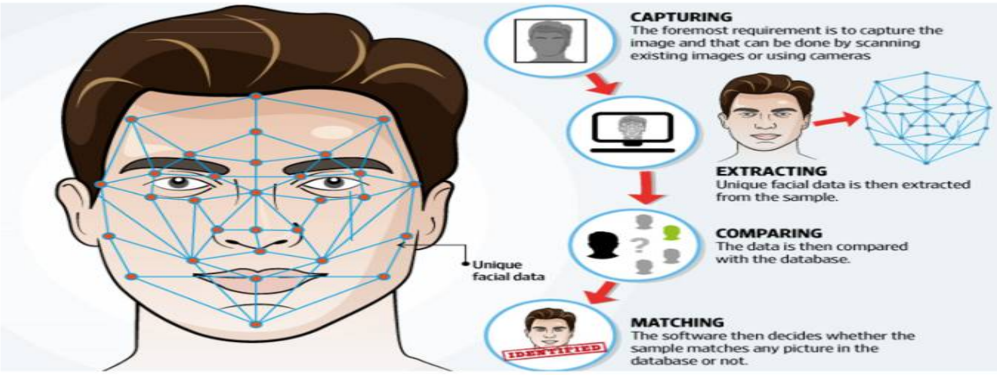
- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

These nodal points are measured creating a numerical code, called a face print, representing the face in the database.

III. HOW FACIAL RECOGNITION WORKS

The face is an important part of who you are and how people identify you. Except in the case of identical twins, the face is arguably a person's most unique physical characteristics. While humans have the innate ability to recognize and distinguish different faces for millions of years, computers are just now catching up. For face recognition there are two types of comparisons .the first is verification. This is where the system compares the given individual with who that individual says they are and gives a yes or no decision. The second is identification. This is where the system compares the given individual to all the Other individuals in the database and gives a ranked list of matches. All identification or authentication technologies operate using the following four stages:

a. Capture: A physical or behavioural sample is captured by the system during
Enrolment and also in identification or verification process
b. Extraction: unique data is extracted from the sample and a template is created.
c. Comparison: the template is then compared with a new sample.
d. Match/non match: the system decides if the features extracted from the new



CAPTURING
The foremost requirement is to capture the image and that can be done by scanning existing images or using cameras

EXTRACTING
Unique facial data is then extracted from the sample.

COMPARING
The data is then compared with the database.

MATCHING
The software then decides whether the sample matches any picture in the database or not.

IV. APPLICATIONS

1. Face Identification:

Face recognition systems identify people by their face images. Face recognition systems establish the presence of an authorized person rather than just checking whether a valid identification (ID) or key is being used or whether the user knows the secret personal identification numbers (Pins) or passwords. The following are example. To eliminate duplicates in a nationwide voter registration system because there are cases where the same person was assigned more than one identification number. The face recognition system directly compares the face images of the voters and does not use ID numbers to differentiate one from the others. When the top two matched faces are highly similar to the query face image, manual review is required to make sure they are indeed different persons so as to eliminate duplicates.

2. Access Control:

In many of the access control applications, such as office access or computer logon, the size of the group of people that need to be recognized is relatively small. The face pictures are also caught under natural conditions, such as frontal faces and indoor illumination. The face recognition system of this application can achieve high accuracy without much co-operation from user. The following are the example. Face recognition technology is used to monitor continuously who is in front of a computer terminal. It allows the user to leave the terminal without closing files and logging out. When the user leaves for a predetermined time, a screen saver covers up the work and disables the mouse & keyboard. When the user comes back and is recognized, the screen saver clears and the previous session appears as it was left. Any other user who tries to logon without authorization is denied

3. Image database investigations:

Searching image databases of licensed drivers benefit recipients, missing children, immigrants and police bookings. General identity verification: Electoral registration, banking, electronic commerce, identifying newborns, national IDs, passports, employee IDs.

4. Financial services:

The financial services industry revolves around the concept of security. Yet for the most part, security within the industry is limited to a simple personal identification number (PIN) or password.

• Biometrics, particularly face recognition software, can improve the security of the financial services industry, saving the institution time and money both through a reduction of fraud cases and the administration expenses of dealing with forgotten passwords.

• Furthermore, biometric-based access control units can safeguard vaults, teller areas, and safety deposit boxes to protect against theft.

• The use of biometrics can also ensure that confidential information remains confidential while deterring identity theft, particularly as it relates to ATM terminals and card-not-present e-commerce transactions

.

5. Security:

Today more than ever, security is a primary concern at airports and for airline staff office and passengers. Airport protection systems that use face recognition technology have been implemented at many airports around the world. The following are the two examples. In October, 2001, Fresno Yosemite International (FYI) airport in California deployed Viisage's face recognition technology for airport security purposes. The system is designed to alert Fly's airport public safety officers whenever an individual matching the appearance of a known terrorist suspect enters the airport's security checkpoint. Anyone recognized by the system would have further investigative processes by public safety officers. Computer security has also seen the application of face recognition technology. To prevent someone else from changing files or transacting with others when the authorized individual leaves the computer terminal for a short time, users are continuously authenticated, checking that the individual in front of the computer screen or at a user is the same authorized person who logged in.

6. Surveillance:

Like security applications in public places, surveillance by face recognition systems has a low user satisfaction level, if not lower. Free lighting conditions, face orientations and other divisors all make the deployment of face recognition systems for large scale surveillance a challenging task. The following are some example of face based surveillance. To enhance town centre surveillance in Newham Borough of London, this has 300 cameras linked to the closed circuit TV (CCTV) controller room. The city council claims that the technology has helped to achieve a 34% drop in crime since its facility. Similar systems are in place in Birmingham, England. In 1999 Visionics was awarded a contract from National Institute of Justice to develop smart CCTV technology.

V. CONCLUSION

Face recognition technologies have been associated generally with very costly top secure applications. Much research effort around the world is being applied to expanding the accuracy and capabilities of this biometric domain, with a consequent broadening of its application in the near future. Verification systems for physical and electronic access security are available today, but the future holds the promise and the threat of passive customization and automated surveillance systems enabled by face recognition.

REFERENCES

1. www.google.com.
2. www.iee.com
3. http://www.Imagestechnology.com
4. www.wikipedia.com
5. Biometrics in Human Services User Group. URL: http://www.dss.state.ct.us/digital.htm.