CHAPTER 1: INTRODUCTION

1.1 CONCEPT OF FACIAL RECOGNITION

Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours. Facial recognition is mostly used for security purposes, though there is increasing interest in other areas of use. In fact, facial recognition technology has received significant attention as it has potential for a wide range of application related to law enforcement as well as other enterprises. There are different facial recognition techniques in use, such as the generalized matching face detection method and the adaptive regional blend matching method. The values measured against the variable associated with points of a person’s face help in uniquely identifying or verifying the person. With this technique, applications can use data captured from faces and can accurately and quickly identify target individuals. Facial recognition techniques are quickly evolving with new approaches such as 3-D modeling, helping to overcome issues with existing techniques.

There are many advantages associated with facial recognition. Compared to other biometric techniques, facial recognition is of a non-contact nature. Face images can be captured from a distance and can be analyzed without ever requiring any interaction with the user/person. As a result, no user can successfully imitate another person. Facial recognition can serve as an excellent security measure for time tracking and attendance. Facial recognition is also cheap technology as there is less processing involved, like in other biometric techniques.

There are certain drawbacks associated with facial recognition. Facial recognition can only identify people when the conditions such as lighting are favourable. The application could be less reliable in case of insufficient light or if the face is partially

obscured. Another disadvantage is that facial recognition is less effective when facial expressions vary.

1.2 CONCEPT OF FINGERPRINT SCANNER

A fingerprint scanner is a type of technology that identifies and authenticates the fingerprints of an individual in order to grant or deny access to a computer system or a physical facility. It is a type of biometric security technology that utilizes the combination of hardware and software techniques to identify the fingerprint scans of an individual.

A fingerprint scanner typically works by first recording fingerprint scans of all authorized individuals for a particular system or facility. These scans are saved within a database. The user requiring access puts their finger on a hardware scanner, which scans and copies the input from the individual and looks for any similarity within the already-stored scans. If there is a positive match, the individual is granted access. Fingerprint scanners most commonly use an individual's thumbprint as identification.

1.3 CONCEPT OF ID TRACKING

Id Tracking refers to a smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card that has embedded integrated circuits. Smart cards can be either contact or contactless smart card. Smart cards can provide personal identification, authentication, data storage, and application processing. Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations.

In virtual space technology, a tracking system is generally a system capable of rendering virtual space to a human observer while tracking the observer's coordinates. For instance, in dynamic virtual auditory space simulations, a real-time head tracker provides feedback to the central processor, allowing for selection of appropriate head-

related transfer functions at the estimated current position of the observer relative to the environment.

1.4 CONCEPT OF IRIS RECOGNITION

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique, stable, and can be seen from some distance. Retinal scanning is a different, ocular-based biometric technology that uses the unique patterns on a person's retina blood vessels and is often confused with iris recognition. Iris recognition uses video camera technology with subtle near infrared illumination to acquire images of the detail-rich, intricate structures of the iris which are visible externally. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual. Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per (single-core) CPU, and with remarkably low false match rates.

Several hundred million persons in several countries around the world have been enrolled in iris recognition systems for convenience purposes such as passport-free automated border-crossings and some national ID programs. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to false matches, is the stability of the iris as an internal and protected, yet externally visible organ of the eye.

1.5 STATEMENT OF THE PROBLEM

Surveys conducted across numerous Industries, Companies, and other organizations throughout the State prove that the employers usually grumble about their current security measures. The primitive methods of industrial security like only watchmen or

security cameras are outdated and hence, the following cases report events that prove them to be less efficient.

Theft at Amazon

Angela Gibson of Kentucky was accused of stealing more than $10,000 in merchandise from Amazon.

Amazon's loss prevention team confronted Gibson, and the police say that she eventually admitted to the theft. When they searched her home, they found more than $10,000 in goods stored in her garage.

This clearly depicts a case of workplace theft and could've been avoided.

Bank employee surrenders

Lisa Wilson was an employee at PMC bank, and is now facing charges of $1,500 in theft. An investigation revealed that between April and September, she was taking money from the daily deposits at the ATM. The bank conducted their own audit and investigation, eventually showing that Wilson was the one responsible.

The 42-year old employee surrendered to the police without incident on Friday, September. They released her on $2,000 unsecured bail to await her hearing.

Utilities employee theft charge

An employee in Freehold, New Jersey who worked as a controller and treasurer for the Middlesex County Utilities Authority was recently arrested for theft in excess of $57,000. The accused, 68-year old Margaret Brennan received charges of theft by deception. She also withdrew money from the utility company's account and wrote checks to herself over the past 2 years.

In all the above cases, the authorities admit that if proper safety/security measures would've been adopted, none of them would have occurred. Thus, companies do need to have a proper, well designed security system to avoid such workplace mishaps.

1.6 AIM AND OBJECTIVES

AIM

To ensure protection of sensitive data and belongings for users and companies in order to increase the security and rectify the flaws in the conventional security systems.

OBJECTIVES

- To bring about fundamental changes as to how the workplace security operates.
- To help minimizing break-ins.
- To protect possessions.
- To know the exact employee allotted to a certain task.
- To avoid workplace theft cases.
- To develop a safe work environment.

CHAPTER 2: REVIEW OF RELATED LITERATURE

2.1 FROM REFERENCE BOOKS/ONLINE JOURNALS

Airport security

Anonymous

December 2015

http://studymafia.org/wp-content/uploads/2015/05/ECE-Face-Recognigion-report.pdf

Airport and other transportation terminal security is not a new thing. People have long had to pass through metal detectors before they boarded a plane, been subject to questioning by security personnel, and restricted from entering "secure" areas. What has changed, is the vigilance in which these security efforts are being applied. The use of biometric identification, can enhance security efforts already underway at most airports and other major transportation hubs (seaports, train stations, etc.). This includes the identification of known terrorists before they get onto an airplane or into a secure location.

Thus we can say that introduction of Biometric system will provide us with maximum security, least legal problems. Biometric systems are ethically acceptable and socially sound. By using these identification techniques we prevent terrorists or criminals from infiltrating a place, moreover preventing any injury or harm to innocent civilians.

Iris Recognition: A Tool for Modern Security

Njoku Leona, Ifunanya

December 2015

http://fruittyblog.blogspot.in/2015/12/a-seminar-report-on-iris-recognition.html

In 1936, ophthalmologist Frank Burch proposed iris pattern for personal recognition. Then in 1987 two ophthalmologists, Aran Safir and Leonard Flom, patented this idea, and they ask John Daugman to create algorithms for iris recognition in 1989 (Daugman,

2001). Iris provides one of the most stable biometric signals for identification, with a distinctive texture that is formed before age one and remains constant throughout life unless there is an injury to the eye (Ives, 2004). Iris recognition can easily be considered as the most reliable form of biometric technology, compared with other biometric technologies, such as face, and fingerprint recognition (Nasser A. Biqami, 2013). Most of the currently deployed commercial algorithms for iris recognition (by John Daugman) have a very low false acceptance rate compared to the other biometric identifiers.

The need for secure methods of authentication is becoming increasingly important in the corporate world today. Our inability to remember complex passwords forgetting PINs all contribute to the possible breakdown in security for an organisation. The uniqueness of the iris and low probability of a false acceptance or false rejection all contribute to the benefits of using iris recognition technology. It provides an accurate and secure method of authenticating users. Users no longer have to worry about remembering passwords and system administrators no longer need to worry about the never-ending problem of users disclosing passwords or having weak passwords that are easily cracked.

2.2 FROM WEBSITES

ATM using fingerprint

Prasaanth

Feb 04, 2012

http://www.seminarsonly.com/forum/atm-using-fingerprint-t3480.html

An embedded Crypto-Biometric authentication scheme for ATM banking systems is proposed in our paper. In this scheme, cryptography and biometric techniques are fused together for person authentication to ameliorate the security level. The fingerprint template including singular points, frequency of ridges and minutiae are stored at the central banking server when enrollment. At the time of transaction fingerprint image is acquired at the ATM terminal using high resolution fingerprint scanner. The fingerprint image is enhanced and then encrypted using 128 bit private key algorithm. The

encrypted image is transmitted to the central server via secured channel. At the banking terminal the image is decrypted using the same key. Based on the decrypted image, minutiae extraction and matching are performed to verify the presented fingerprint image belongs to the claimed user. The authentication is signed if the minutiae matching are successful. The proposed scheme is fast and more secure. Computer simulations and statistical analysis are presented.

It cannot be denied that the data provided by fingerprint image can be convenient, helpful, reliable as well as secure when it comes to ATM related transactions. Fingerprint recognition is an emerging field and it paves way for the researchers to invent new methods to reduce the error rates and to improve the accuracy and speed of the system

CHAPTER 3: SCOPE

3.1 ADDITIONAL USES OF FACIAL RECOGNITION

3.1.1 To make online payments

We all know a hassle online payments can be creating an account, adding your shipping and billing addresses, putting in your credit card. Not to mention how nerve wracking it can often be to give up such personal information to a website.

3.1.2 Gaming

Image and face recognition is bringing a whole new dimension to gaming. Microsoft's Kinects advanced motion sensing capabilities have given the Xbox 360 a whole new lease of life and opened up gaming to new audiences by completely doing away with hardware controllers.

3.2 ADDITIONAL USES OF FINGERPRINT SCANNER

3.2.1 Transaction

If the ATM Machine and Card may connect with the UID card system then only allowed people would transact money Authenticate by Fingerprint Scanner at ATM.

3.2.2 Election Duty

If the Government Election may conduct using UID card, then fake entries can be avoided.

3.3 ADDITIONAL USES OF IRIS SCANNER

- While the most common use of iris recognition to date is physical access control in private enterprise and government, the versatility of the technology will lead

to its growing use in large sectors of the economy such as transportation, healthcare, and national identification programs.

- This growing need, as well as Iris ID competence in iris technology, coupled with core interests in IT and wireless, provides the impetus for design efforts for the future and mas Iris ID the one to watch for new developments in identity management tomorrow and beyond.

3.4 ADDITIONAL USES OF ID TRACKING

3.4.1 Electronic Purse

A smart card can be used to store a monetary value for small purchases. Card readers retrieve the amount currently stored, and subtract the amount for the goods or services being purchased. Groceries, transportation tickets, parking, Laundromats, cafeterias, taxis and all types of vending machines.

3.4.2 ID Verification And Access Control

The computational power of smart cards allows running mutual authentication and public-key encryption software in order to reliably identify the bearer of the card. For higher security needs, a smart card is a tamper-proof device to store such information as a user's picture or fingerprints. Smart cards can be used also for network access: in addition or in alternative to user IDs and passwords, a networked computer equipped with a smart card reader can reliably identify the user.

CHAPTER 4: DESIGN

4.1 FACIAL RECOGNITION CAMERA

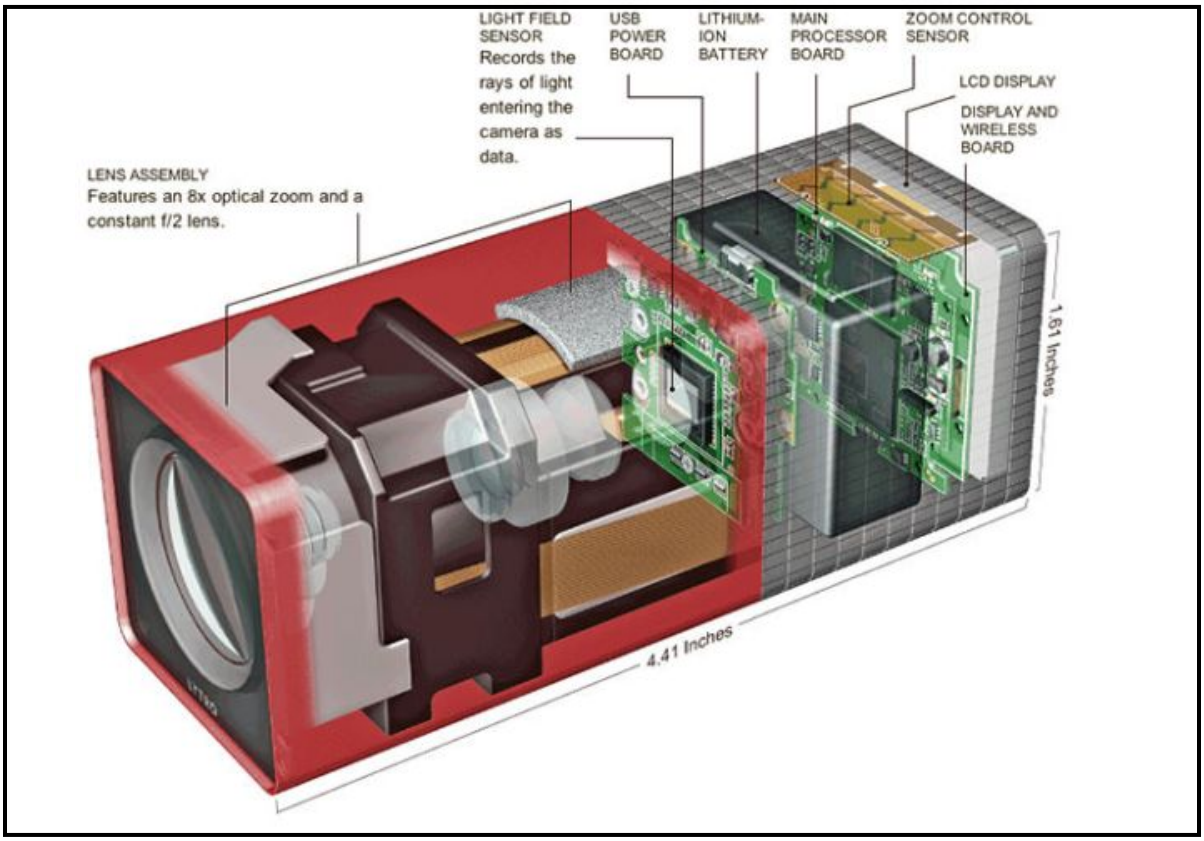

Fig. no. 4.1: Facial Recognition Camera

4.1.1 Parts

- Lens are used in conjunction with a camera body and mechanism to make images of objects either on photographic film or on other media capable of storing an image chemically or electronically.
- DVR(Digital Video Recorder) record and stores the images or videos sent by the CCTV(Closed Circuit television) cameras
- Monitor is used to reproduce the image or video created by the camera
- Zoom lenses can be remotely adjusted to allow variation of the focal length.

4.1.2 Features

- Used for recognizing different faces at workplace
- Used to record images and video

- Sending an alert message unknown face is been scanned
- 3D sensors to capture information about the shape of a face.
- The Thermal cameras will only detect the shape of the head and it will ignore the subject accessories such as glasses, hats, or make up.

4.2 IRIS RECOGNITION

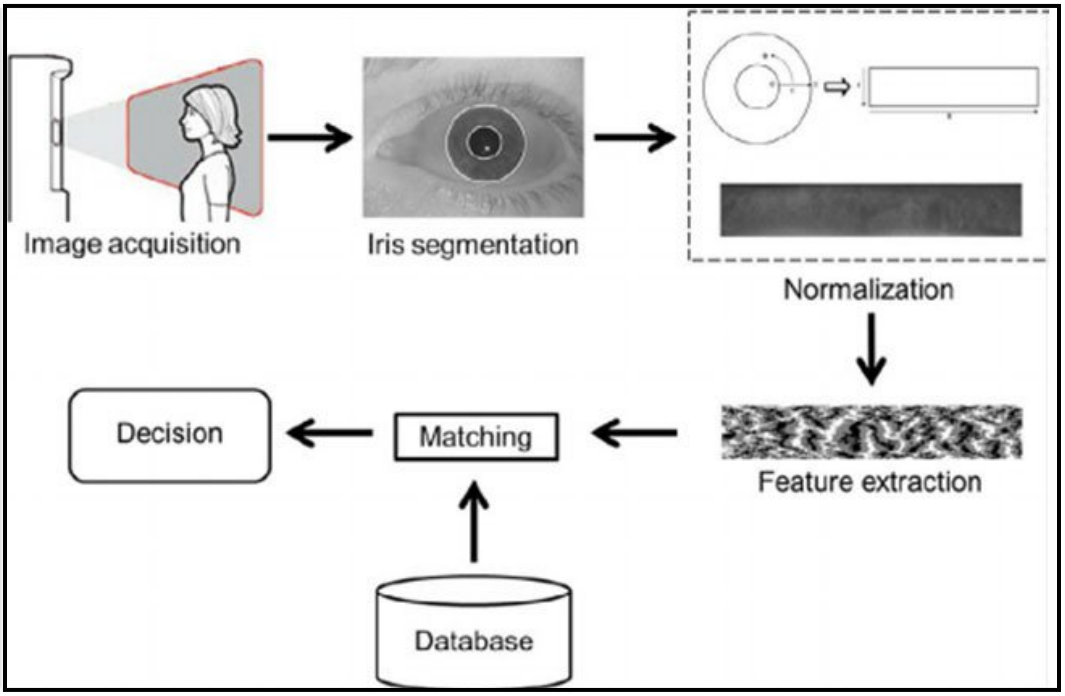

Fig. no. 4.2: IrisRecognition

4.2.1 Parts

- Scanner are used for scanning center of the pupil, edge of the pupil,the edge of the iris.the eyelids and eyelashes
- Camera scans the person's eye and produces a digital image
- Feature extraction is used to extract the outer and inter circle or iris.

4.2.2 Features

- Used for higher security reasons.
- Mostly used at the main entrance of the working place.
- Secure access to any accounts
- High-levels of safety against identity theft

4.3 FINGERPRINT SCANNER

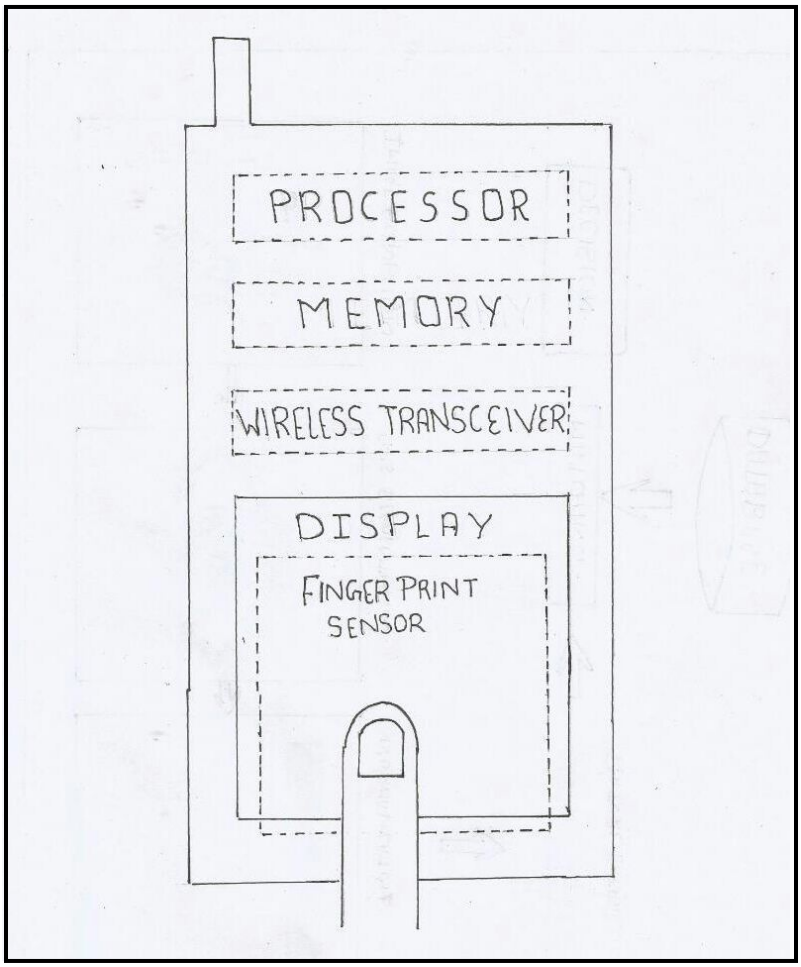

Fig. no. 4.3: Fingerpring scanner

4.3.1 Parts

- A fingerprint sensor captures a digital image of a fingerprint pattern
- light source is used to illuminate the finger's surface
- charge-coupled device (CCD) captures the digital image
- Optical sensor technology creates patterns and images using light

4.3.2 Features

- Fingerprint scanners are unique and highly secure.
- They are easier , cheaper and faster to setup.
- Fingerprint Scanner offers very high accuracy.

4.4 ID TRACKER

4.4.1 Parts

- GPS tracker device fits into the identity card and captures the location.

- GPS tracking server has three responsibilities: receiving data from the GPS tracking unit, securely storing it, and serving this information on demand to the user.

4.4.2 Features

- You can track all the route made by the employee graphically on the map.
- Anytime anywhere access.
- It get deactivated after certain distance outside the company.
- Remains activate only in the Company area.
- Gives accurate location of the employee.

CHAPTER 5: IMPLEMENTATION

5.1 FACIAL DETECTION SYSTEM

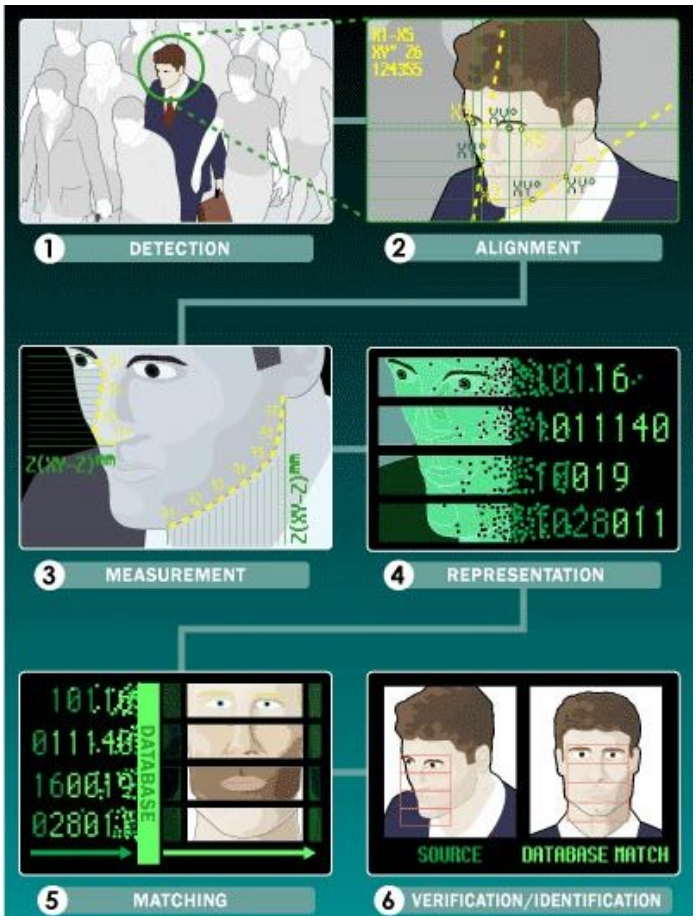

Fig. no. 5.1: Facial Recognition System

The image that is to e compared with the database is obtained either as a photo [2-D] or as a video image [3-D].

For a 2-D image, the system can be accurate only if the angular position of the face towards the camera is at least 35 degrees. But for a 3-D image, the system can be accurate even if the angular position of the face towards the camera is at 90 degrees. The size and pose can also affect the accuracy.

The face recognition software makes templates on the different curves of the face. The face will be measured in micrometer scales.

The software used for facial recognition recognizes and distinguishes the face from its background by some of the common nodal points given below.

- Distance between the eyes
- Nose width
- Depth of the eye sockets
- Cheekbone shape
- Length of jaw-line

The above nodal points are measured altogether to provide a common numerical code known as the face print.

The measurement taken is then transferred into a unique code. This code makes each template unique and thus represents the different features of the face.

The comparison of the image with the database can occur in two ways. If both the image taken and the image in the database are 3-D, then there is no problem in the matching process.

The comparison can be classified into two according to its purpose. One of them is verification and the other is identification.

If a person is to be identified as one who claims to be an employee of a particular office, it is called verification. This type of comparison will with the database will only take place in a 1:1 ratio.

For the identification of a thief or a culprit, the image received will be compared to all the images in the database in a 1: N ratio.

5.2 IRIS SCANNER

A camera scans the person's eye and produces a digital image.

Image processing software attempts to isolate the iris by drawing two circles, one at its inner boundary (between the pupil and the iris) and the other at its outer boundary (known as the limbus, between the iris and the white, outer sclera). The inner boundary is relatively easy to detect, because it's generally a circle with a sudden change in brightness where the pupil gives way to the iris. A broadly similar process is used to find the outer boundary, though it has to allow for the likelihood of the eyelids blocking part of the iris.

Polar coordinates (concentric circles and radial lines from their origin) are then added to the image to define separate "zones of analysis," so that key features of the iris can be accurately located and compared in two-dimensional space. This system cleverly allows for the way the iris changes as the pupil grows (dilates) and shrinks (constricts) in different light conditions.

The pattern of light and dark areas in the iris is then converted into digital form using bandpass filters (crudely speaking, if the brightness in a given area is more than a certain amount, the filters might register a 1, otherwise they would register a 0), and, with a bit of mathematical juggling, this generates the unique, digital IrisCode®. A particular eye will generate roughly the same code whether its pupil is dilated or not.

5.3 FINGERPRINT SCANNER

A row of LEDs scans bright light onto the glass (or plastic) surface on which your finger is pressing. The quality of the image will vary according to how you're pressing, how clean or greasy your fingers are, how clean the scanning surface is, the light level in the room, and so on.

Reflected light bounces back from your finger, through the glass, onto a CCD or CMOS image sensor. The longer this image-capture process takes, the brighter the image formed on the image sensor.

If the image is too bright, areas of the fingerprint (including important details) may be washed out completely—like an indoor digital photo where the flash is too close or too bright. If it's too dark, the whole image will look black and details will be invisible for the opposite reason.

An algorithm tests whether the image is too light or too dark; if so, an audible beep or LED indicator alerts the operator and we go back to step 1 to try again.

If the image is roughly acceptable, another algorithm tests the level of detail, typically by counting the number of ridges and making sure there are alternate light and dark areas (as you'd expect to find in a decent fingerprint image). If the image fails this test, we go back to step 1 and try again.

Providing the image passes these two tests, the scanner signals that the image is OK to the operator (again, either by beeping or with a different LED indicator). The image is stored as an acceptable scan in flash memory, ready to be transmitted (by USB cable, wireless, Bluetooth, or some similar method) to a host computer where it can be processed further. Typically, images captured this way are 512×512 pixels (the dimensions used by the FBI), and the standard image is 2.5cm (1 inch) square, 500 dots per inch, and 256 shades of gray.

The host computer can either store the image on a database (temporarily or indefinitely) or automatically compare it against one or many other fingerprints to find a match.

5.4 ID TRACKER (RFID TRACKER)

A Radio-Frequency identification system has three parts:

- A scanning antenna
- A transceiver with a decoder to interpret the data
- A transponder - the RFID tag - that has been programmed with information.

The scanning antenna puts out radio-frequency signals in a relatively short range. The RF radiation does two things:

a. It provides a means of communicating with the transponder (the RFID tag)

b. It provides the RFID tag with the energy to communicate (in the case of passive RFID tags).

When an RFID tag passes through the field of the scanning antenna, it detects the activation signal from the antenna. That "wakes up" the RFID chip, and it transmits the information on its microchip to be picked up by the scanning antenna.

The activated chip can then be used to transmit the location of the employee and thus, helping the employer to know about the task being allocated/performed by the employee.

CHAPTER 6: ANALYSIS

Now a day passwords are not secure and some time as a useless as an access control at least that is what many vendors and security consultants try to tell managers today. Instead, these purveyors of change claim that biometrics solves all password issues and improves productivity.

6.1 ADVANTAGES TO THE BANK

- While traditional security systems are reliant on passwords, personal identification numbers (PINs) or smart cards, we can achieve a high level of accuracy with biometrics systems. If you have set up the system correctly, these features cannot be easily duplicated, which means only the authorized person gets access and you get high level of security.

- Biometric logins creates a clear, definable audit trail of transactions or activities. This is especially handy in case of security breaches because we know exactly who is responsible for it. As a result we get true and complete accountability, which cannot be duplicated.

6.2 ADVANTAGES TO THE PUBLIC

- The good thing about using biometrics for identification is that modern systems are built and designed to be easy and safe to use. Biometrics technology gives us accurate results with minimal invasiveness as a simple scan or a photograph is usually all that's required. Moreover the software and hardware can be easily used and we can have them installed without the need for excessive training.

- Biometric identification is extremely quick, which is another advantage it has over other traditional security methods. A person can be identified or rejected in a matter of seconds.

- For those business owners that understand the value of time management the use of this technology can only be beneficial to your office revenue by increasing productivity and reducing costs by eliminating fraud and waste.

- We can have biometrics systems installed rather easily and after that, they do their job quickly, reliably and uniformly. We will need only a minimum amount of training to get the system operational and there is no need for expensive password administrators. If we use high quality systems, it will also mean our maintenance costs are reduced to minimize the expenses of maintaining an ongoing system.

6.3 ADVANTAGES TO SECURITY ASPECTS

- Another advantage these systems have is that they can't be guessed or stolen; hence they will be a long term security solution our company. The problem with efficient password systems is that there is often a sequence of numbers, letters, and symbols, which makes difficult to remember on a regular basis.

6.4 LIMITATIONS

- Unlike passwords and cryptographic keys that are known only to the user, biometrics such as face and fingerprints can easily be recorded and potentially misused by biometrics experts without the user's consent.
- Biometrics cannot be cancelled such as Passwords, PINs, etc can be recover or reset if compromised. But biometrics is permanently associated with the user and cannot be replaced if compromised.
- Biometrics provides usability advantages since it obviates the need to remember and manage multiple passwords..
- It is likely that the same biometric might be used for various applications and locations, the user can potentially be tracked if organizations collude and share their respective biometric databases while traditional authentication schemes requires the user to maintain different identities to prevent tracking.

CHAPTER 7: SUGGESTIONS FOR FURTHER STUDY

The further study can be done in such aspect that it may be possible that future application for facial recognition systems lies in retailing.

Example: A retail grocery store may have cash registers equipped with cameras; the cameras would be aimed at the faces of customers, so pictures of customers could be obtained. The camera would be the primary means of identifying the customer, and if visual identification failed, the customer could complete the purchase by using a PIN (personal identification number).

After the cash register had calculated the total sale, the face recognition system would verify the identity of the customer and the total amount of the sale would be deducted from the customer's bank account. Hence, face-based retailing would provide convenience for retail customers, since they could go shopping simply by showing their faces, and there would be no need to bring debit cards, or other financial media. Wide reaching applications of face based retailing are possible, including retail stores, restaurants, movie theaters, car rental companies, hotels, etc. e.g. Swiss European surveillance: facial recognition and vehicle make, model, color and license plate reader.

Indeed, if automatic devices for identity recognition were more prevalent in locations such as airports, police stations and other areas that are sensitive or involve high concentrations of public activity, they would surely make the life of criminals and terrorists much more difficult. However, there are many reasons to believe that biometrics will change the life of people in near future mostly because its use will be much more convenient than other techniques in use today for individual identity authentication. This is already apparent today, especially in connection with applications such as physical and logical access control, transportation, and also in the financial industry.

Authentication:

It is reasonable to expect, that in a relatively short time, all personal documents will contain some form of biometric data. Moreover, in time, we could expect that all such documents will no longer be needed, because, in every instance where this type of authentication would be necessary, biometric readers will be connected to the location via network. This would allow a comparison with stored data to be used in lieu of documentation.

Access and attendance control:

In the relatively near future, biometrics will certainly gain increased acceptance in all kinds of access and attendance control applications. We can expect to see biometrics used for these applications in homes, offices, computers, machines, devices, etc. However, for the most part, the use of these devices will only replace existing access control methods and technologies, providing increased convenience and security. There will be no need to carry keys, identity cards, personal documents, etc.

Action control:

At the last place where one would specify a market that can be seen as a part of previous ones but it has special features and can require specific devices. In the case of potentially dangerous devices it is necessary or would be good to control the use of them to prevent that unauthorized people can use them or to track, who has used them in a specific situation.

REFERENCES

BIBLIOGRAPHY

[1] Gene Kim, Jez Humble, Patrick Debois, and John Willis. '*The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*'

[2] Lisa Laskow Lahey, Matthew L. Miller, and Robert Kegan. '*An Everyone Culture: Becoming a Deliberately Developmental Organization*'

[3] Matt Pascucci. '*Extrusion Detection: Security Monitoring for Internal Intrusions*'

[4] Stan Z. Li, Anil Kumar Jain. '*Handbook of Face Recognition, 2nd Edition*'

WEBLIOGRAPHY

- http://www.martinpi.com/5-recent-cases-of-workplace-theft/
- http://www.makeuseof.com/tag/technology-explained-how-do-rfid-tags-work/
- http://science.howstuffworks.com/biometrics4.htm
- http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/nn3page1.stm
- https://en.wikipedia.org/wiki/Security_awareness