

INTRODUCTION

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances.

Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords: birthdays, phone numbers and social security numbers. Recent cases of identity theft have hightened the nee for methods to prove that someone is truly who he/she claims to be.

Face recognition technology may solve this problem since a face is undeniably connected to its owner expect in the case of identical twins. Its nontransferable. The system can then compare scans to records stored in a central or local database or even on a smart card.

What are biometrics?

A biometric is a unique, measurable characteristic of a human being that can be used to automatically recognize an individual or verify an individual's identity. Biometrics can measure both physiological and behavioral characteristics. Physiological biometrics (based on measurements and data derived from direct measurement of a part of the human body) include:

- Finger-scan
- Facial Recognition
- Iris-scan
- Retina-scan
- Hand-scan

Behavioral biometrics (based on measurements and data derived from an action) include:

- Voice-scan
- Signature-scan
- Keystroke-scan

A "biometric system" refers to the integrated hardware and software used to conduct biometric identification or verification.

Why we choose face recognition over other biometric?

There are a number reasons to choose face recognition. This includes the following

1. It requires no physical interaction on behalf of the user.
2. It is accurate and allows for high enrolment and verification rates.
3. It does not require an expert to interpret the comparison result.
4. It can use your existing hardware infrastructure, existing cameras and image capture devices will work with no problems.
5. It is the only biometric that allow you to perform passive identification in a one to many environment (eg: identifying a terrorist in a busy Airport terminal).

FACE RECOGNITION

THE FACE:

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:

- capture: a physical or behavioural sample is captured by the system during enrollment and also in identification or verification process.
- Extraction: unique data is extracted from the sample and a template is created.
- Comparison: the template is then compared with a new sample.
- Match/non match : the system decides if the features extracted from the new sample are a match or a non match.

Face recognition technology analyze the unique shape ,pattern and positioning of the facial features. Face recognition is very complex technology and is largely software based. This Biometric Methodology establishes the analysis framework with tailored algorithms for each type of biometric device. Face recognition starts with a picture, attempting to find a person in the image. This can be accomplished using several methods including movement, skin tones, or blurred human shapes. The face recognition system locates the head and finally the eyes of the individual. A matrix is then developed based on the characteristics of the individual's face. The method of defining the matrix varies according to the algorithm (the mathematical process used by the computer to perform the comparison). This matrix is then compared to matrices that are in a database and a similarity score is generated for each comparison.

Artificial intelligence is used to simulate human interpretation of faces. In order to increase the accuracy and adaptability , some kind of machine learning has to be implemented.

There are essentially two methods of capture. One is video imaging and the other is thermal imaging. Video imaging is more common as standard video cameras can be used. The precise position and the angle of the head and the surrounding lighting conditions may affect the system performance. The complete facial image is usually captured and a number of points on the face can then be mapped, position of the eyes, mouth and the nostrils as a example. More advanced technologies make 3-D map of the face which multiplies the possible measurements that can be made. Thermal imaging has better accuracy as it uses facial temperature variations caused by vein structure as the distinguishing traits. As the heat pattern is emitted from the face itself without source of external radiation these systems can capture images despite the lighting condition, even in the dark. The drawback is high cost. They are more expensive than standard video cameras.

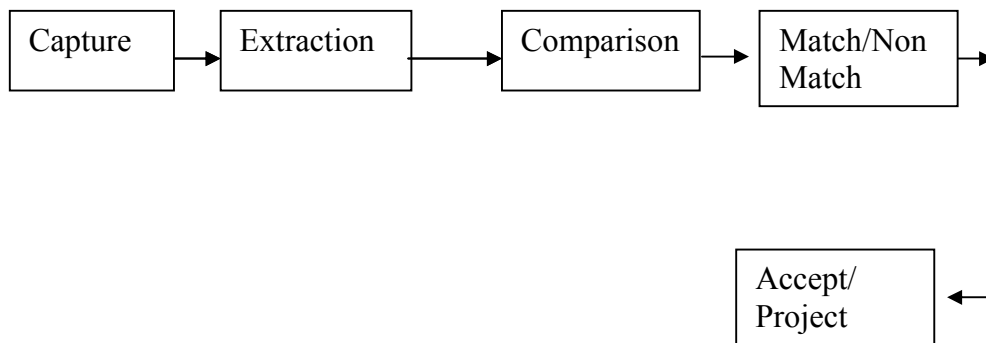


Figure 1

CAPTURING OF IMAGE BY STANDARD VIDEO CAMERAS

The image is optical in characteristics and may be thought of as a collection of a large number of bright and dark areas representing the picture details. At an instant there will be large number of picture details existing simultaneously each representing the level of brightness of the scene to be reproduced. In other words the picture information is a function of two variables: time and space. Therefore it would require infinite number of channels to transmit optical information corresponding to picture elements simultaneously. There are practical difficulty in transmitting all information simultaneously so we use a method called scanning.

Here the conversion of optical information to electrical form and its transmission is carried out element by element one at a time in a sequential manner to cover the entire image. A TV camera converts optical information into electrical information, the amplitude of which varies in accordance with variation of brightness.

An optical image of the scene to be transmitted is focused by lense assembly on the rectangular glass plate of the camera tube. The inner side of this has a transparent coating on which is laid a very thin layer of photoconductive material. The photolayer has very high resistance when no light is falling on it but decreases depending on the intensity of light falling on it. An electron beam is formed by an electron gun in the TV camera tube. This beam is used to pick up the picture information now avilable on the target plate of varying resistace at each point.

The electron beam is deflected by a pair of deflecting coils mounted on the glass envelope and kept mutually perpendicular to each other to achieve scanning of the entire target area. The deflecting coils are fed separately from two sweep oscillators, each operating at different frequencies. The magnetic deflection caused by current in one coil gives horizontal motion to the beam from left to right at a uniform rate and brings it back to the left side to commence the trace of the next line. The other coil is used to deflect the beam from top to bottom.

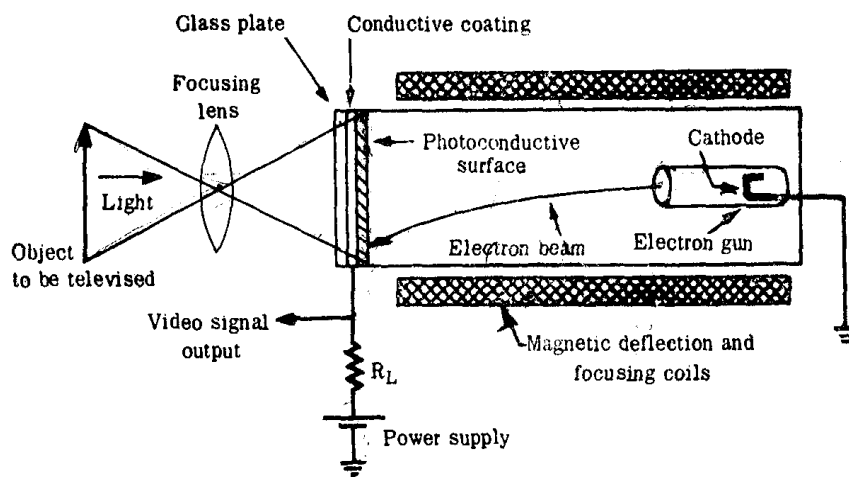
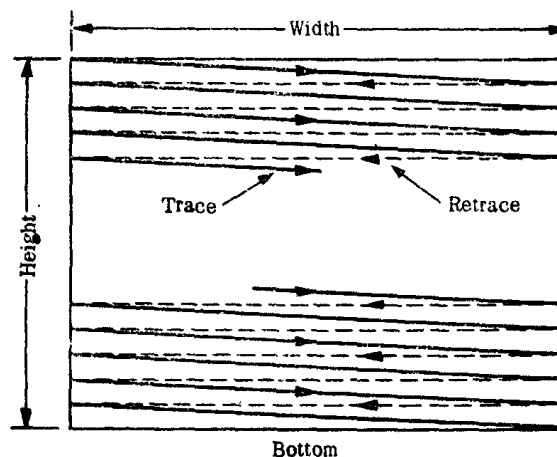


Figure 2

Top



Bottom

Figure 3.

As the beam moves from element to element it encounters different resistance across the target plate depending on the resistance of the photoconductive coating. The result is flow of current which varies in magnitude as elements are scanned. The current passes through the load resistance R_l connected to conductive coating on one side of the DC supply source on the other. Depending on the magnitude of current a varying voltage appears across the resistance R_l and this corresponds to the optical information of the picture

COMPONENTS OF FACE RECOGNITION SYSTEMS

- An automated mechanism that scans and captures a digital or an analog image of a living personal characteristics.(enrollment module)
- Another entity which handles compression, processing, storage and compression of the captured data with stored data (database)
- The third interfaces with the application system (identification module)

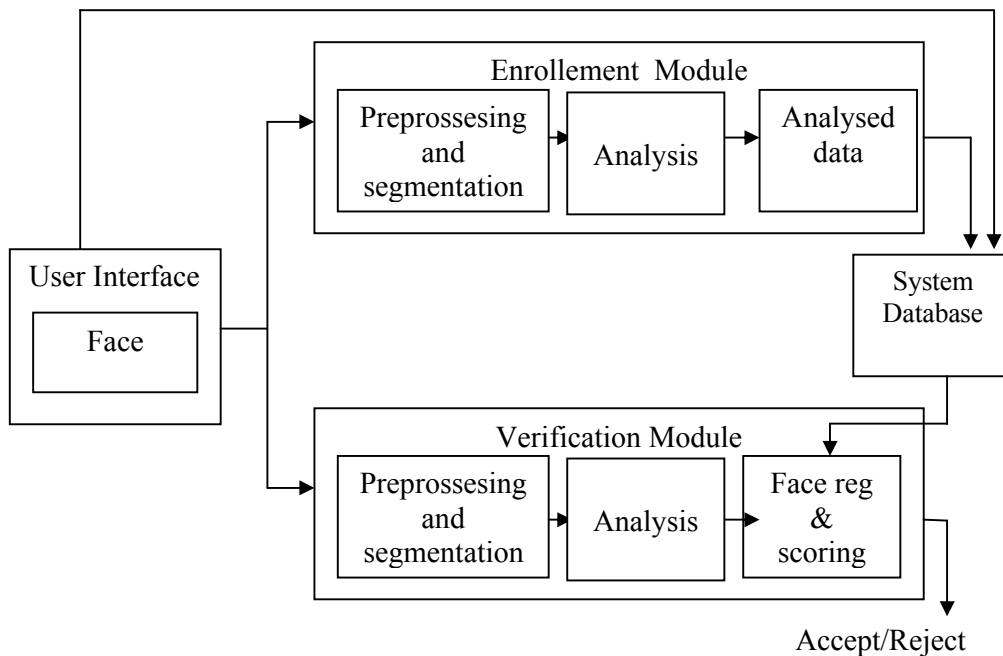


Figure 4

User interface captures the analog or digital image of the person's face. In the enrollment module the obtained sample is preprocessed and analyzed. This analyzed data is stored in the database for the purpose of future comparison.

The database compresses the obtained sample and stores it. It should have retrieval property also that is it compares all the stored sample with the newly obtained sample and retrieves the matched sample for the purpose of verification by the user and determine whether the match declared is right or wrong.

The verification module also consists of a preprocessing system. Verification means the system checks as to who the person says he or she is and gives a yes or no decision. In this module the newly obtained sample is preprocessed and compared with the sample stored in the database. The decision is taken depending on the match obtained from the database. Correspondingly the sample is accepted or rejected.

Instead of verification module we can make use of identification module. In this the sample is compared with all the other samples stored in the database. For each comparison made a match score is given. The decision to accept or reject the sample depends on this match score falling above or below a predetermined threshold.

PERFORMANCE

- False acceptance rate (FAR)

The probability that a system will incorrectly identify an individual or will fail to reject an imposter. It is also called as type 2 error rate.

$$FAR = NFA / NIIA$$

Where FAR= false acceptance rate
NFA= number of false acceptance
NIIA= number of imposter identification attempts

- False rejection rates (FRR)

The probability that a system will fail to identify an enrollee. It is also called type 1 error rate

$$FRR = NFR / NEIA$$

Where FRR= false rejection rates
NFR= number of false rejection rates
NEIA= number of enrollee identification attempt

- Response time:

The time period required by a biometric system to return a decision on identification of a sample.

- Threshold/ decision Threshold:

The acceptance or rejection of a data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the system can be made more or less strict; depending on the requirements of any given application.

- Enrollment time:

The time period a person must spend to have his/her facial reference template successfully created.

- Equal error rate:

When the decision threshold of a system is set so that the proportion of false rejection will be approximately equal to the proportion of false acceptance. This synonym is 'crossover rate'. The facial verification process involves computing the distance between the stored pattern and the live sample. The decision to accept or reject is dependent on a predetermined threshold. (Decision threshold).

IMPLEMENTATION OF FACE RECOGNITION TECHNOLOGY

The implementation of face recognition technology include the following four stages:

- data acquisition
- input processing
- face image classification and decision making

Data acquisition:

The input can be recorded video of the speaker or a still image. A sample of 1 sec duration consists of a 25 frame video sequence. More than one camera can be used to produce a 3D representation of the face and to protect against the usage of photographs to gain unauthorized access.

Input processing:

A pre-processing module locates the eye position and takes care of the surrounding lighting condition and colour variance. First the presence of faces or face in a scene must be detected. Once the face is detected, it must be localized and normalization process may be required to bring the dimensions of the live facial sample in alignment with the one on the template.

Some facial recognition approaches use the whole face while others concentrate on facial components and/ or regions(such as lips, eyes etc). the appearance of the face can change considerably during speech and due to facial expressions. In particular the mouth is subjected to fundamental changes

but is also very important source for discriminating faces. So an approach to persons recognition is developed based on spatio-temporal modeling of features extracted from talking face. Models are trained specific to a persons speech articulate and the way that the person speaks. Person identification is performed by tracking mouth movements of the talking face and by estimating the likelihood of each model of having generated the observed sequence of features. The model with the highest likelihood is chosen as the recognized person.

Block diagram:

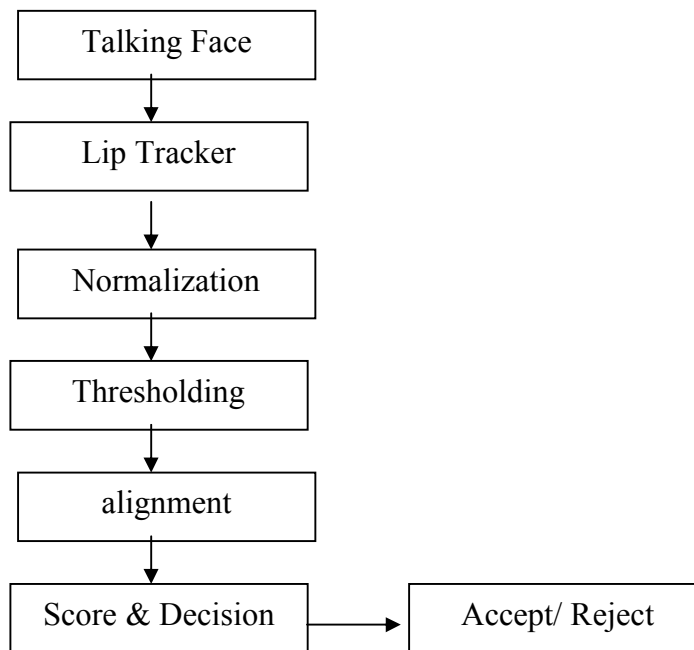


Figure 5

Face image classification and decision making:

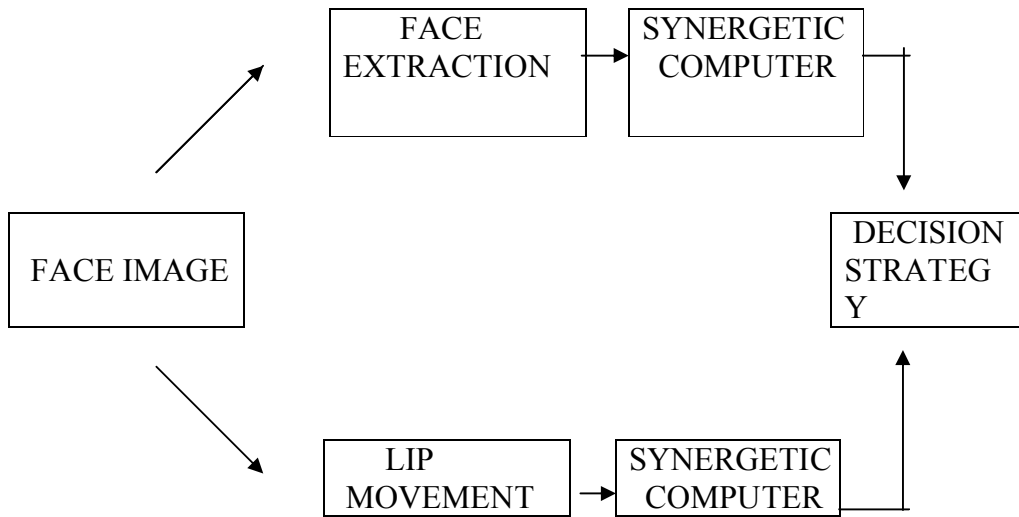


Figure 6

Synergetic computer are used to classify optical and audio features, respectively. A synergetic computer is a set of algorithm that simulate synergetic phenomena. In training phase the BIOID creates a prototype called faceprint for each person. A newly recorded pattern is preprocessed and compared with each faceprint stored in the database. As comparisons are made, the system assigns a value to the comparison using a scale of one to ten. If a score is above a predetermined threshold, a match is declared.

From the image of the face, a particular trait is extracted. It may measure various nodal points of the face like the distance between the eyes ,width of nose etc. it is fed to a synergetic computer which consists of algorithm to capture, process, compare the sample with the one stored in the database. We can also track the lip movements which is also fed to the

synergetic computer. Observing the likelihood each of the sample with the one stored in the database we can accept or reject the sample.

HOW FACE RECOGNITION SYSTEMS WORK

An example

Visionics, company based in a New Jersey is one of the many developers of facial recognition technology. The twist to its particular software, Face it is that it can pick someone's face from the rest of the scene and compare it to a database full of stored images. In order for this software to work, it has to know what a basic face looks like. Facial recognition software is based on the ability to first recognize faces, which is a technological feat in itself and then measure the various features of each face.

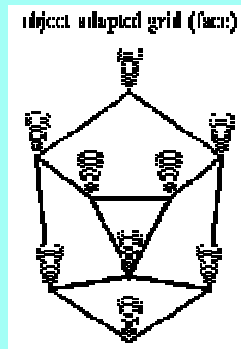


If you look at the mirror, you can see that your face has certain distinguishable landmarks. These are the peaks and valleys that make up the different facial features. Visionics defines these landmarks as nodal points.

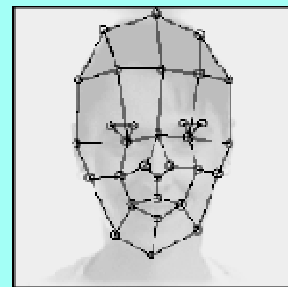
There are about 80 nodal points on a human face. Here are few nodal points that are measured by the software.

- distance between the eyes
- width of the nose
- depth of the eye socket
- cheekbones
- jaw line
- chin

A face bunch graph is created from 70 face models to obtain a general representation of the face



Given an image the face is matched to the face bunch graph to find the fiducial points



An image graph is created using elastic graph matching and compared to database of faces for recognition

Figure 7

These nodal points are measured to create a numerical code, a string of numbers that represents a face in the database. This code is called

faceprint. Only 14 to 22 nodal points are needed for faceit software to complete the recognition process.

THE SOFTWARE

Facial recognition software falls into a larger group of technologies known as biometrics. Facial recognition methods may vary, but they generally involve a series of steps that serve to capture, analyze and compare your face to a database of stored images. Here is the basic process that is used by the Faceit system to capture and compare images:

Detection

When the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for faces. If there is a face in the view, it is detected within a fraction of a second. A multi-scale algorithm is used to search for faces in low resolution. (An algorithm is a program that provides a set of instructions to accomplish a specific task). The system switches to a high-resolution search only after a head-like shape is detected.

Alignment

Once a face is detected, the system determines the head's position, size and pose. A face needs to be turned at least 35 degrees toward the camera for the system to register it.

Normalization

The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose. Normalization is performed regardless of the head's location and distance from the camera. Light does not impact the normalization process.

Representation

The system translates the facial data into a unique code. This coding process allows for easier comparison of the newly acquired facial data to stored facial data.

Matching

The newly acquired facial data is compared to the stored data and (ideally) linked to at least one stored facial representation. The heart of the FaceIt facial recognition system is the Local Feature Analysis (LFA) algorithm. This is the mathematical technique the system uses to encode faces. The system maps the face and creates a faceprint, a unique numerical code for that face. Once the system has stored a faceprint, it can compare it to the thousands or millions of faceprints stored in a database. Each faceprint is stored as an 84-byte file. Using facial recognition software, police can zoom in with cameras and take a snapshot of a face.



The system can match multiple faceprints at a rate of 60 million per minute from memory or 15 million per minute from hard disk. As comparisons are made, the system assigns a value to the comparison using a scale of one to 10. If a score is above a predetermined threshold, a match is declared. The operator then views the two photos that have been declared a match to be certain that the computer is accurate.

ADVANTAGES AND DISADVANTAGES

Advantages:

1. There are many benefits to face recognition systems such as its convenience and social acceptability. All you need is your picture taken for it to work.
2. Face recognition is easy to use and in many cases it can be performed without a person even knowing.
3. Face recognition is also one of the most inexpensive biometric in the market and its prices should continue to go down.

Disadvantage:

1. Face recognition systems can't tell the difference between identical twins.

APPLICATIONS

The natural use of face recognition technology is the replacement of PIN, physical tokens or both needed in automatic authorization or identification schemes. Additional uses are automation of human identification or role authentication in such cases where assistance of another human needed in verifying the ID cards and its beholder.

There are numerous applications for face recognition technology:

Government Use

1. Law Enforcement: Minimizing victim trauma by narrowing mugshot searches, verifying identify for court records, and comparing school surveillance camera images to known child molesters.
2. Security/Counterterrorism. Access control, comparing surveillance images to known terrorists.
3. Immigration: Rapid progression through Customs.

Commercial Use

1. Day Care: Verify identity of individuals picking up the children.
2. Residential Security: Alert homeowners of approaching personnel.
3. Voter verification: Where eligible politicians are required to verify their identity during a voting process. this is intended to stop 'proxy' voting where the vote may not go as expected.
4. Banking using ATM: The software is able to quickly verify a customers face .
5. Physical access control of buildings areas ,doors, cars or net access.

CONCLUSION

Face recognition technologies have been associated generally with very costly top secure applications. Today the core technologies have evolved and the cost of equipments is going down dramatically due to the intergration and the increasing processing power. Certain application of face recognition technology are now cost effective, reliable and highly accurate. As a result there are no technological or financial barriers for stepping from the pilot project to widespread deployment.

BIBLIOGRAPHY

1. ELECTRONICS FOR YOU- Part 1 April 2001
Part 2 May 2001
2. ELECTRONIC WORLD - DECEMBER 2002
3. MODERN TELEVISION ENGINEERING- Gulati R.R
4. IEEE INTELLIGENT SYSTEMS - MAY/JUNE 2003
5. WWW.FACEREG.COM
6. WWW. IMAGESTECHNOLOGY.COM
7. WWW.IEEE.COM

ABSTRACT

Wouldn't you love to replace password based access control to avoid having to reset forgotten password and worry about the integrity of your system? Wouldn't you like to rest secure in comfort that your healthcare system does not merely rely on your social security number as proof of your identity for granting access to your medical records?

Because each of these questions is becoming more and more important, access to a reliable personal identification is becoming increasingly essential. Conventional methods of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised. But a face is undeniably connected to its owner. It cannot be borrowed, stolen or easily forged.

CONTENTS

- 1. INTRODUCTION**
- 2. FACE RECOGNITION**
- 3. CAPTURING OF IMAGE BY STANDARD VIDEO
CAMERAS**
- 4. COMPONENTS OF FACE RECOGNITION SYSTEMS**
- 5. PERFORMANCE**
- 6. IMPLEMENTATION OF FACE RECOGNITION
TECHNOLOGY**
- 7. HOW FACE RECOGNITION SYSTEMS WORK -An
example**
- 8. THE SOFTWARE**
- 9. ADVANTAGES AND DISADVANTAGES**
- 10. APPLICATIONS**
- 11. CONCLUSION**
- 12. REFERENCES**

ACKNOWLEDGEMENT

I extend my sincere gratitude towards **Prof . P.Sukumaran** Head of Department for giving us his invaluable knowledge and wonderful technical guidance

I express my thanks to **Mr. Muhammed kutty** our group tutor and also to our staff advisor **Ms. Biji Paul** for their kind co-operation and guidance for preparing and presenting this seminar.

I also thank all the other faculty members of AEI department and my friends for their help and support.