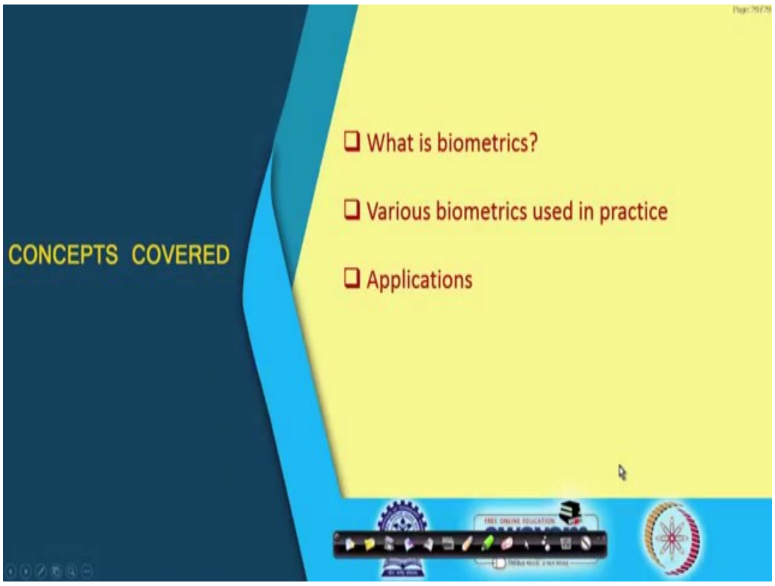
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technologies, Kharagpur

Lecture – 37
Biometric Authentication

In our earlier lectures, we have seen the various security primitives out of which authentication was one of the most important requirements.

Now, once the message is being transferred or transmitted over the network, you need to authenticate the two parties. But there are applications where some person has to be authenticated. The person has to be present in that place and you have to verify whether that person is indeed the individual who he or she is claiming to be; this is what is referred to as Biometric Authentication and this is the topic of this lecture.

(Refer Slide Time: 01:09)



CONCEPTS COVERED

□ What is biometrics?

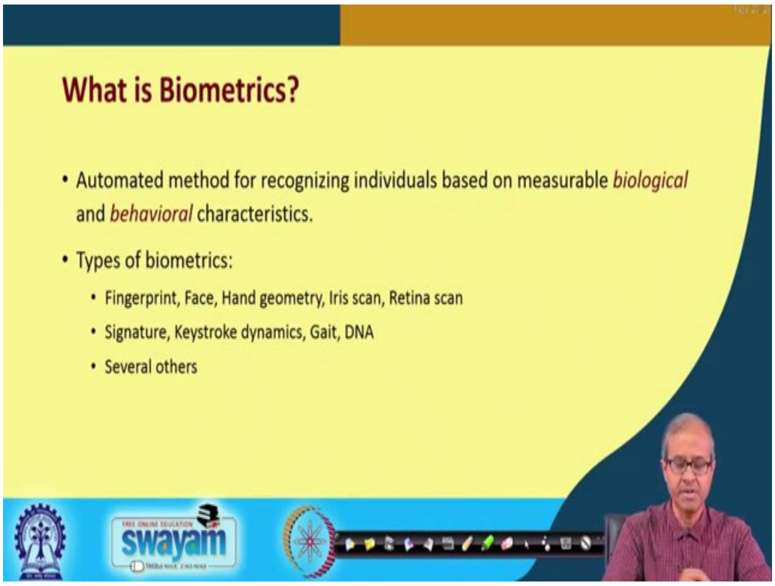
□ Various biometrics used in practice

□ Applications

Now, in this lecture without going into the detail of the techniques and technologies, we shall provide you with an overview of what is biometrics? What are the various biometric traits that are used in practice and some of the applications? Now, in biometrics one thing you just understand that as it is said that the person whom you are authenticating has to be present physically in the place where this authentication is carried out.

So, what are you authenticating? You should authenticate some direct physical or psychological properties of that person, how he looks, his or her fingerprint, how he walks and so on; these are a few things which are typically used.

(Refer Slide Time: 02:01)



What is Biometrics?

- Automated method for recognizing individuals based on measurable *biological* and *behavioral* characteristics.
- Types of biometrics:
  - Fingerprint, Face, Hand geometry, Iris scan, Retina scan
  - Signature, Keystroke dynamics, Gait, DNA
  - Several others

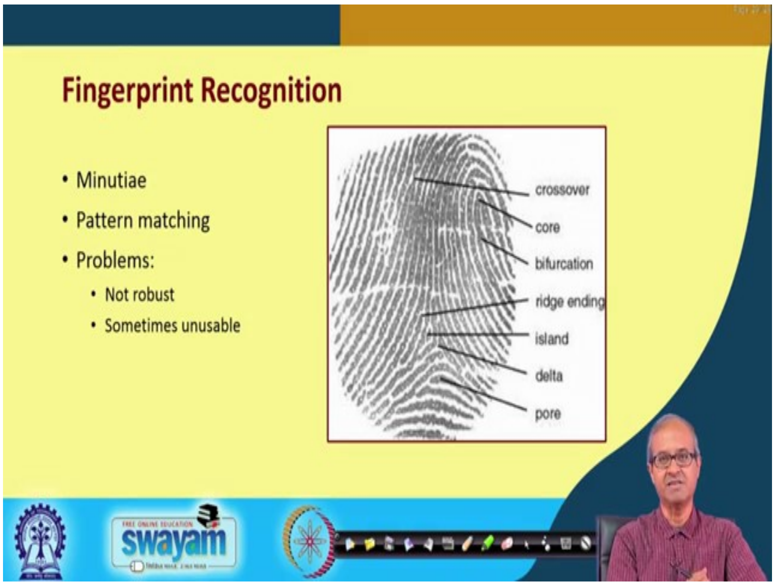
Let us see the basic definition of biometrics. Biometric is defined as some automated method for recognizing individuals; this is the basic idea. But how we can do it? Based on some measurable biological or behavioral characteristics; or a combination of both; there can be several biological or behavioral characteristics that you may need to look at.

Some of the typical features which people have explored include fingerprint which is very commonly used, you know. Face recognition; face, hand geometry like hand. Every hand is unique like, how much gap is there between two fingers, what is the geometry, what are the lengths? There are many features there and also some marks or lines in the hands; these are called hand geometry; this is also a very unique way of identifying a person.

Iris scan, the center of your eye is called iris. You can scan an iris, there are some systems where this iris is used as biometric or you can scan your entire retina. The entire eye, the retina that is more accurate than iris. And some of your behavioral features like your signature, how you sign; create a signature and when you are typing on the keyboard; what are your features, just two persons will have some difference in the way they type, ok, keystroke dynamics.

Gait means how you walk; two persons their walking style will be distinctly different. And of course, DNA is one of the biological properties; DNA of a person is supposed to unique, but of course, DNA checking cannot be done instantaneously; it takes much longer time and there are several others. So, you may use any one of them and if you want more robust and more accurate system; you can use multiple of them together.

(Refer Slide Time: 04:23)



Fingerprint Recognition

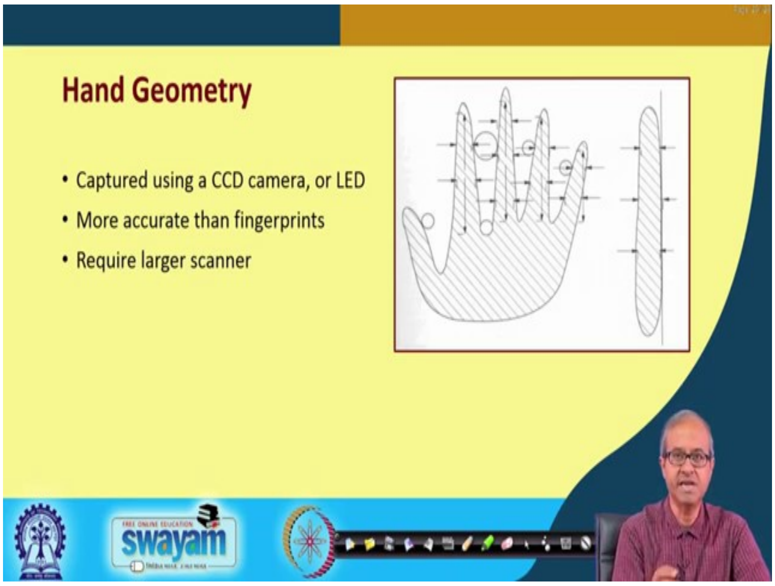
- Minutiae
- Pattern matching
- Problems:
  - Not robust
  - Sometimes unusable

Let us look at some of these one by one; fingerprint recognition; you have seen fingerprint readers in many places; I am sure. Fingerprint recognition is it, it essentially, it looks at the tiny lines and curves and edges and ridges that are present in the fingers; tips of the fingers. And there are some terms which are used crossover, cores, bifurcation, ridge ending, island, delta, pore; you identify where exactly in your fingerprint image these are located; these are called minutiae.

So, these places where there is a sudden change, these are called minutiae points; you identify the minutiae points and you can detect these features in your fingerprint. So instead of storing in the entire fingerprint image, you can identify these and you can compress it into a very small quantity and by comparison you can actually identify a person. So, there will be some kind of a pattern matching, but the problem is, this method is not very robust; like in terms of fingerprinting, you have to have a very clear fingerprint to have good detection probability, ok.

Sometimes, you may see, you may have to put your fingers several times before you are getting authenticated. And if there is some dirt on your finger or some ink or there is some dirt on the surface where you are putting your finger on, there can be some error in scanning; so sometimes it may not be usable. So, this fingerprint recognition is certainly one of the very popularly used methods, but this is not really a failsafe method. Well, you can use fingerprinting at some doors for to gain entry into a premise, but you cannot use fingerprint for your bank transaction because it is not considered to be 100 percent safe.

(Refer Slide Time: 06:35)



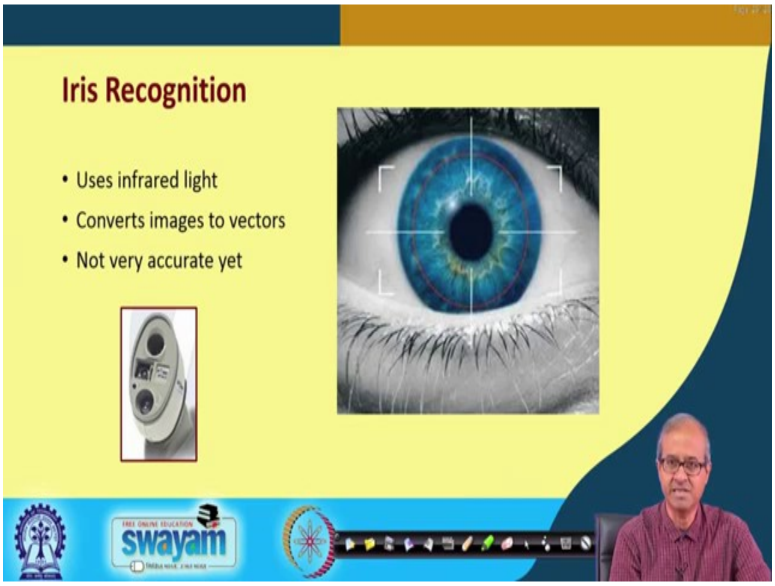
Hand Geometry

- Captured using a CCD camera, or LED
- More accurate than fingerprints
- Require larger scanner

Well, I said hand geometry carries lot of information like what are the lengths of your fingers, what are the gaps between the fingers, shapes of the fingers and if you look at the side view, side view what is, what is the geometry? So, there are lots of features in your hand which are unique and also some marks on your hand that also can be seen in general. These are more accurate than fingerprints, but the problem is that to put your hand, you need a larger scanner.

A fingerprint scanner will be very small, let us say about a inch in size, but hand scanner needs to be very large.

(Refer Slide Time: 07:15)



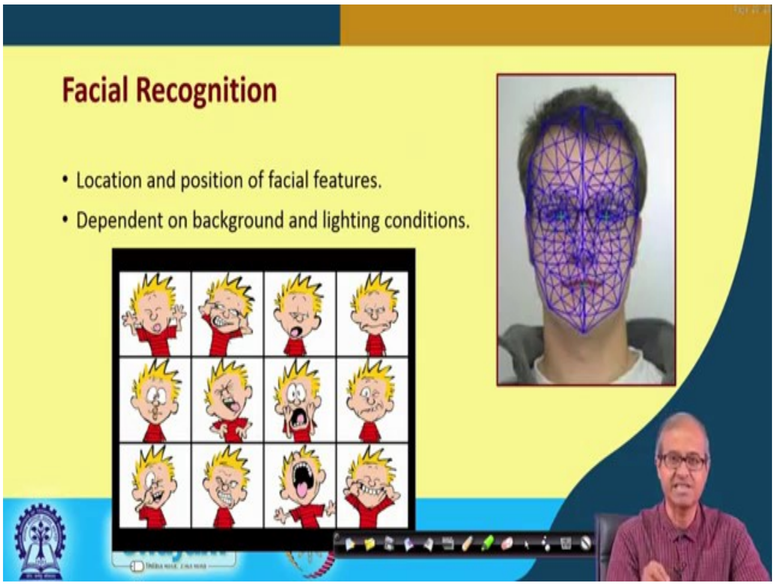
Iris Recognition

- Uses infrared light
- Converts images to vectors
- Not very accurate yet

When iris as I said; iris cognition is something which is used in several places. The central part of your eye, this is called the iris and there are some cameras which is specifically designed to capture your iris recognition. So, these cameras use infrared light; one of these is an infrared source and the other is a camera and after capturing the image, the image is typically converted into vectors.

And well, this also is moderately accurate; it is also not very foolproof. There can be some errors in validation or authentication even using iris.

(Refer Slide Time: 08:03)



Facial Recognition

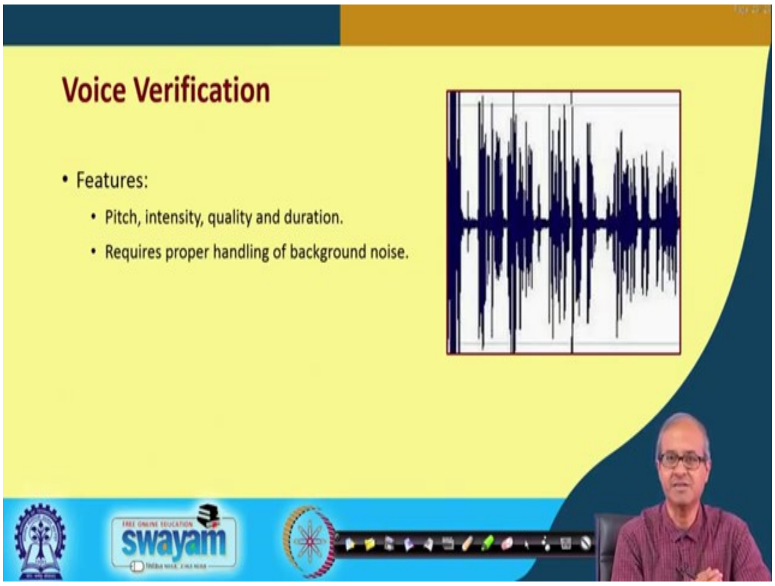
- Location and position of facial features.
- Dependent on background and lighting conditions.

Facial recognition is considered to be better provided you get a good image of your face. You can see, you can see the eye; you can see the nose; you can see the ears; you can see the chin; there are so many features in a face, ok. If you take the image of a complete picture, then the location and the position of facial features can uniquely identify a person. But of course, as you can understand, the image must be made available in some restricted environment like proper background, proper lighting and so on.

Like while you are providing a photograph in many places like a passport application for example, or visa application; you are often asked to provide your picture in a specific format; in a light background, clear, face should be visible and so on, ok. But another thing is that the expression of the face; when you are actually taking the picture for detection, for identification that also makes an important. I have a cartoon here; so you see the same person can make so many different faces; so this is also a challenge.

So, there can be variations; so your detection mechanism should be robust against at least some of the variation; these are extreme variations of course, this is just a cartoon.

(Refer Slide Time: 09:33)



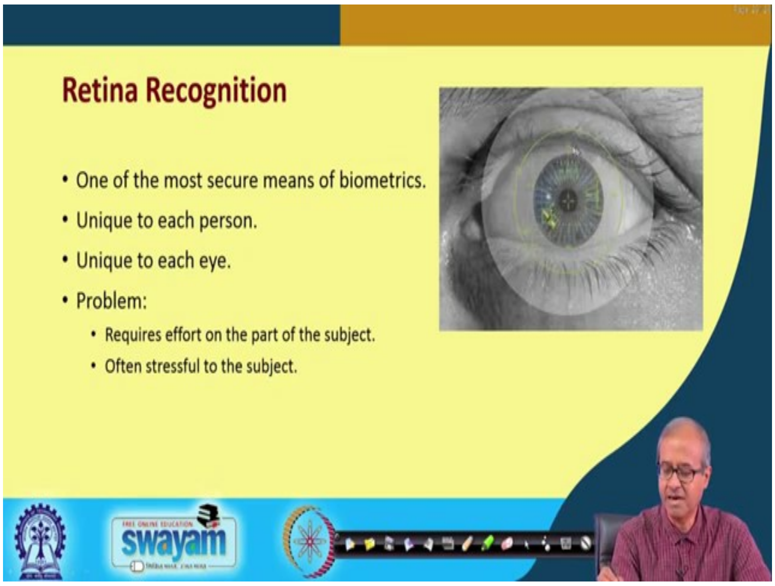
Voice Verification

- Features:
  - Pitch, intensity, quality and duration.
  - Requires proper handling of background noise.

Voice is another very important biometric trait which have been explored; suppose I speak on a microphone. I will get identified. Because the way I speak, there are some very specific features with respect to the pitch intensity and quality of my voice, also in duration, ok; so voice verification also is very important.

There are many applications where you can activate some devices using your voice and only you can activate; if we, if someone else talks and instructs that will not be recognized. So, that device have, will have the intelligence to identify the features of your voice and identify yourself from your voice. But again it is not a general vocabulary or speaking, but certain specific commands, stop, go, up, down something like that you are speaking and the system is identifying it uniquely.

(Refer Slide Time: 10:39)



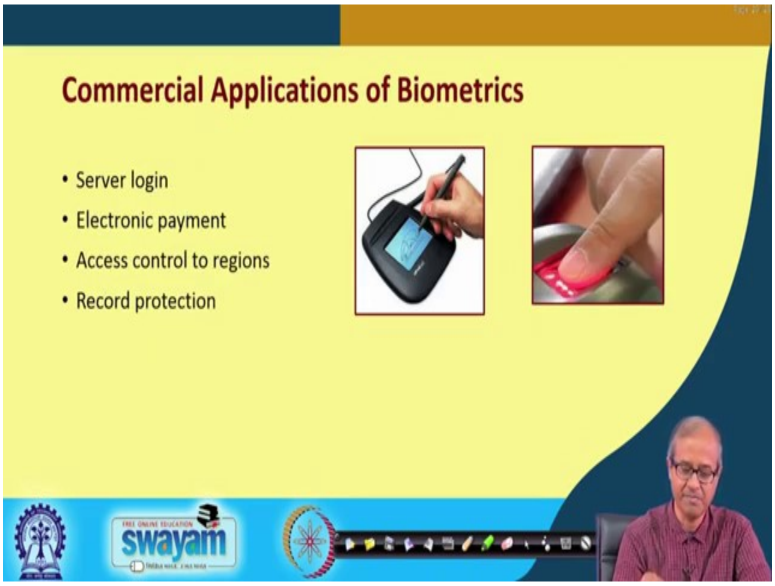
Retina Recognition

- One of the most secure means of biometrics.
- Unique to each person.
- Unique to each eye.
- Problem:
  - Requires effort on the part of the subject.
  - Often stressful to the subject.

Retina as I said, retina involves much larger region of your eye and that is much more, much more accurate as compared to iris. And retina is supposed to be unique to each person and even unique to each eye; the two eyes, the retinas will be different.

This method is pretty accurate, but the problem is that when you want to take the image of a retina; you have to open your eyes; open and you have to stare at a camera for a longer time which may be a little annoying and stressful to the person who you are scanning for recognition. So, taking the retina image is a little troublesome; this is the only downside of this method.

(Refer Slide Time: 11:31)



Commercial Applications of Biometrics

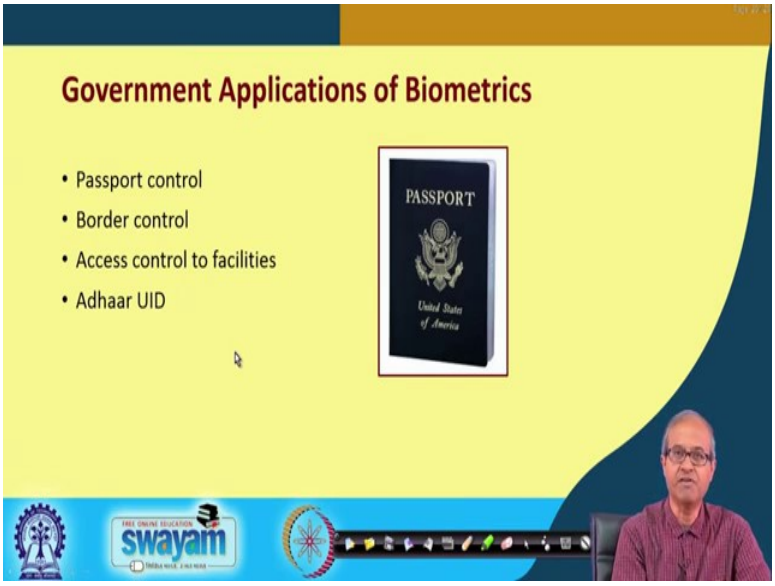
- Server login
- Electronic payment
- Access control to regions
- Record protection

So, talking about the typical application; there are many commercial applications you can think of. Well you log in to a server; there can be some biometric also like you think of a mobile phone that is like your personal server.

There are newer mobile phones, modern mobile phone where you can unlock the screen by using your fingerprint for example, or user, using your face. There are such schemes available. Then electronic payment, there are many electronic payment gateway where some kind of biometric authentication is required. Access control to region, you want to enter a room, enter a laboratory, enter a building; you may have to show your face, give your fingerprint, something like that.

Record protection; suppose you have some records if some information, confidential information stored somewhere; when you want to update it, you have to verify that it is actually you; you can again put some kind of biometric authentication in place before you can carry out that identification, ok; here is some of the examples.

(Refer Slide Time: 12:47)

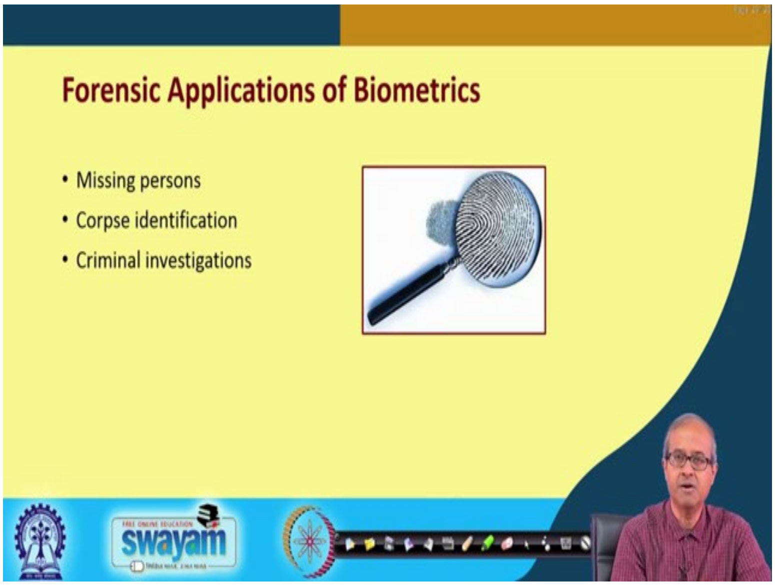


Government Applications of Biometrics

- Passport control
- Border control
- Access control to facilities
- Adhaar UID

Talking about government application, there are many such applications you already know of. Passport control, visa applications, there you use border control that is visa, access control to facilities; government building some very secure places and Adhaar UID which we are all familiar with now that is also an initiative by the government that again uses a set of biometrics to uniquely identify a person, ok; these are some of the attempts.

(Refer Slide Time: 13:19)



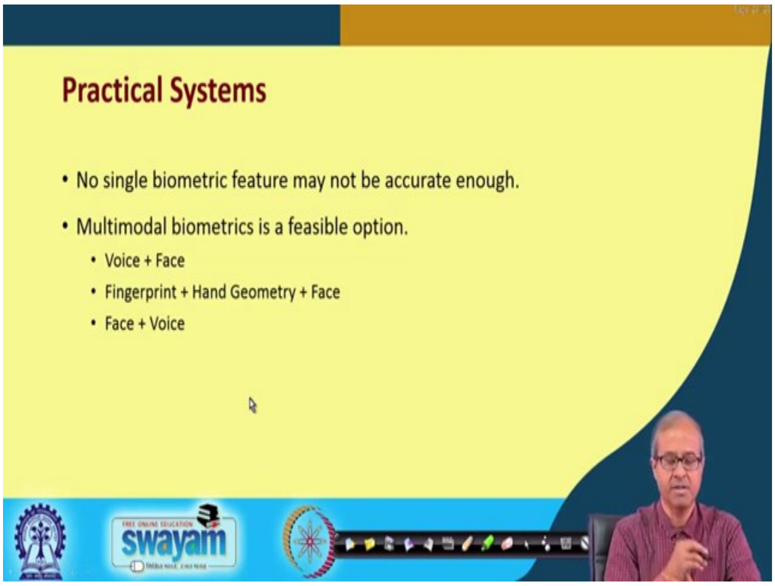
Forensic Applications of Biometrics

- Missing persons
- Corpse identification
- Criminal investigations

Of course, a very big application is in forensics. Well, when some crime has happened; usually the forensic experts go to the site and try to look for fingerprints; so that is one way. And also you can identify some missing persons using some kind of biometric; maybe the person has lost his or her senses, not able to remember; there is a loss of memory.

So, you can check some kind of biometric trace to identify that person; some cops you are not able to identify a dead body, you can use biometrics and of course, criminal investigation I have already told, there are many applications in fact.

(Refer Slide Time: 14:07)



Practical Systems

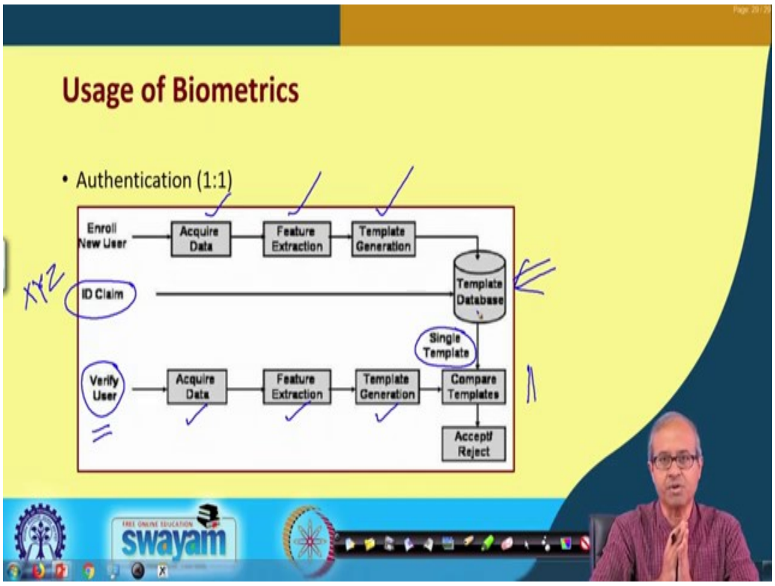
- No single biometric feature may not be accurate enough.
- Multimodal biometrics is a feasible option.
  - Voice + Face
  - Fingerprint + Hand Geometry + Face
  - Face + Voice

Now, talking about practical systems as I said no single system is 100 percent foolproof. So, you normally should have a combination of two or three important biometric traits to uniquely identify a person right; this is called multimodal biometrics.

Let us say you can have a combination of voice and face; you can have a combination of fingerprint, hand geometry and face; face, ok; face and voice sentence is repeated anyway, so you can have any combination of these. So, as I told you, practical system should have some kind of better detection probability; identification probability and single biometric take may not give you that, you should use multiple or more than one.

But again this can be one level of security; if you are talking about some very sensitive applications you may need to add some added level of security on top of this.

(Refer Slide Time: 15:15)



Usage of Biometrics

- Authentication (1:1)

Enroll New User

Acquire Data

Feature Extraction

Template Generation

Template Database

XYZ

ID Claim

Single Template

Verify User

Acquire Data

Feature Extraction

Template Generation

Compare Templates

Accept/ Reject

Now, broadly speaking there are two ways in which you can use biometric for identification. One is; one is to one which is authentication like I am saying that I am Mister XYZ, the system should identify that I am XYZ. So, the idea is that I am sitting here; this is where I am sand, standing and this is my claim; I am saying that I am Mister XYZ. So, what was done earlier? Earlier all the users in the system were enrolled, data acquisition was carried out.

Suppose it was fingerprint, so all the fingerprints were acquired, some features, the minutiae points and the features are extracted from the images and some basic template for each user was generated and these templates were stored in a database. So, when I say, I am mister XYZ; then the template corresponding to mister XYZ would be extracted that would be a single template and I am standing here. So, I will again present my fingerprint, my data will be acquired, feature will extracted, template will be generated and there will be a template matching carried out here.

So, template matching will be one to one; my template will be matched against that single template taken out from the database whether they are matching or not. If they match, then the system will say that well actually I am XYZ; it otherwise will say that there is no match, you are not XYZ, ok; this is for authentication. But suppose you think of a scenario that the biometric information of all the criminals in a state are stored in a database. Now, you catch hold of a suspect; something has happened; you catch hold of somebody; you try to find out whether that person is one of those criminals whose database is there.

So, now you have to compare one person against maybe 1000 persons or more than that stored in the database. This will be a more time consuming process. So, this is the second approach. This is the verification approach. You say one is to N. So, a person is available whom we want to verify against all store templates in the database. So, it is not that you are comparing one with one, but one with many and you just believe there will never be an exact match because biometric traits are such that there will only be a partial match.

So, how much match you will consider as a match and below how much will be considered as a mismatch that is of course, up to experimentation. So, these are the broadly two approaches in which you can use this kind of biometrics. So, with this we come to the end of this lecture; now in this lecture essentially we talked very briefly about the concept of biometrics; how it is being used for access control.

Now, the reason I chose to discuss this is that in any security system nowadays whenever you want to secure your organizational network, you will find that there are many places where entry is granted using some kind of biometrics. You have to be very much aware of the kind of levels of accuracy and the different ways of hacking these systems so that you can have a better idea about how to secure your system in terms of ethical hacking and security testing of your system.

Thank you.