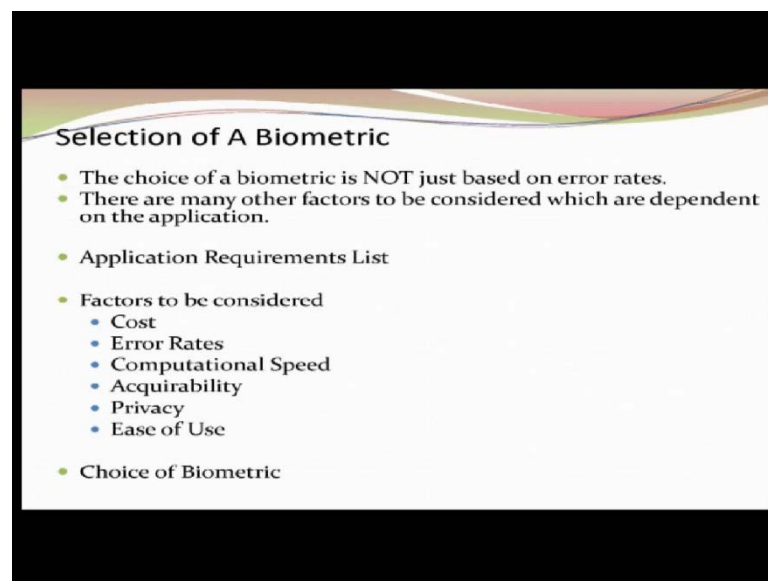


Biometrics
Prof. Phalguni Gupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture No. # 14

(Refer Slide Time: 00:18)



Selection of A Biometric

- The choice of a biometric is NOT just based on error rates.
- There are many other factors to be considered which are dependent on the application.
- Application Requirements List
- Factors to be considered
 - Cost
 - Error Rates
 - Computational Speed
 - Acquirability
 - Privacy
 - Ease of Use
- Choice of Biometric

So, how to select a biometrics state? Which biometrics state will be useful for our activity? So, one way till now what we understood that there are false acceptance rate, there are false rejection rate or equal error rate; these informations are known to you or you have the threshold, for these threshold you have the different $f_{a r l}$ and $f_{r l}$ and based on that you would like to select a biometric state. But that is not a correct way only error is not a sufficient thing there are several other issues.

Now, first part you have to keep it in mind that what for you are introducing the biometrics device or biometrics state? That has to be known to you. What is the application? Why you like to use it? What you are going to gain throughout from this? All those things to be studied carefully.

So, you need to know what are the requirements and specifications, where you are going to implement. Suppose, I want to implement for this classroom; I know this classroom

size is 100, there are two doors and one door will not be opened. Suppose, it may so happen that every chair I keep one biometric device and you sit and give your finger print. But is it worth that 100 100 biometric finger prints scanner I am putting it for a classroom of size 100 and each cost 8000 rupees or so.

So what is the value? How many of us will be using it? What I will be gaining? All those things to be studied. So, the requirement is the most important part you have to understand. And once you know the requirement there are few factors you have to keep analyze carefully; first one is of course, is the cost. Because, if it is 8000 rupees and 100 chairs for the classroom it is very costly thing, because it is 8 hours lectures and for that 8 hours 100 students.

Suppose, my classroom is full and you will find that I will give only one finger print which takes 10 seconds. So, 10 seconds 8 class for each finger print it will be used only 80 seconds rest of the period it is idle. The cost verses time will be a problem. Then, error rates of course error rates will be a because you have to understand the depth of the security you are looking for, based on that you have to select what type of error rates is acceptable for you.

Then speed; how much time it takes to accept the data to analyze the data and so on is it acquirable that, suppose I use thus a sensor for cultivators, finger print sensor then it may so happen the most of the time it is not accepting the data. So acquirability is that issue then privacy is most important. Whatever, data I am giving you how safe it is? It is completely known to the system only not others and is it easy to use?

For example, in the classroom if I think that no I take Iris data. You will find that it takes you or four finger print data it takes lot of time it is not easy to use. Whereas, if I take the face photograph, nobody will be disturbed I will take automatically your photographs without your knowledge also. And then, the the manager or the industry employer; they have also biased us with respect to the system.

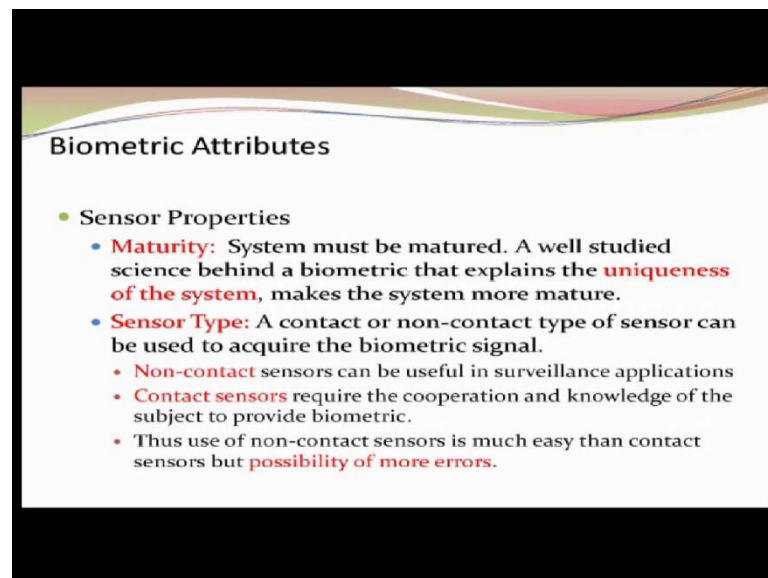
Recently, one party came and they wanted to use the biometry system. I asked what for? They told that it is for the recruitment purpose. Then, I told fine then but it is a finger print is sufficient for you or you take the signature this is sufficient for you, take the photograph sufficient for you. But this man is biased towards Iris he is giving the pressure no no we want to use the Iris I do not know what for you want to use the Iris

there is no value because he **he** understands from the book that Iris gives you the best results.

In the case of recruitment say if I take the fingerprint or the face photograph that is sufficient. Why I am claiming to I explained to him see that, I take the photograph and then it is not final that he just appearing a written test you take his photograph and you will be getting enough chance to monitor him. Because, after that if he clears his entrance test then, you will be calling for interview again you take the photograph.

Then even if he clears it then again at a time of joining also you can take his photograph. So, you have enough time to monitor that candidate, so Iris is not required. But he said no **no**. So, this is a important parameter that not only all these factors that peoples mentality also important.

(Refer Slide Time: 05:57)



Now, once you understand that for any biometric state you need a sensor. So, you have to understand the what is the property of the sensor? Is it matured enough? What does it mean? The matured enough means that, it is stable for or it is well accepted the sensor is well accepted by the society for long time and there is enough **enough** research has gone has been done to draw the conclusion that this sensor this type of sensor gives you the unique characteristics.

So that is the important thing. So this is the most important component is the maturity. See for example, it is true for any **any** hardware devices you purchase. It is not only this biometric sensor. Suppose, we like to procure the system 300 p c(s) for our lab, what we do? Procedure is that first we will go for the manufactures that and check what are the new p c(s) available new type of available.

Now, we do not go for the most recent one. Because, we do not know how much robust it is. Because, if it fails then my 300 p c gone and my money will be in problem. So, what we do? We take the one level below which is already stable people understand that yes it is been studied and people you accepted and then you are taking it. And, not only it gives you the idea of the robust thing also you are getting the idea of the cost, because as the time goes the cost of the system will also goes down.

So, one level minus is the appropriate way of selecting, because the maturity is the issue. Now, since that type is the next one now you decide the system because, employers they always give the pressure that, I want the system of this type. Is it the contact one or it is the non contact one? That means what? That contact one means that I have to touch the sensor to give my biometrics data. And in that process, if I have to touch it then I did the my cooperation I have to give full cooperation to give my biometric data. And, also that the people will be knowing that I am collecting your bio data or collecting your biometrics. So, this is the truth one thing. That first thing in that in the contact thing is that I need the full cooperation from the subject.

Second thing is that the subject will know that I am collecting your biometrics information(s) and non contact is that it is not required you may know, may not know I am collecting your data for example, I have put the surveillance camera and you are coming and I am taking your photographs, without informing you or after informing you.

Now the contact lens sensors are very easy. They are just I am putting it and I am taking your photograph one by one and so on. But there are 2 factors involved in that; one is that it gives lot of errors compared to **compared to** the contact one; another one is that it involves lot of cost. Say for example, I put that you have a p t z camera here know in front of your entry point, have you seen that camera?

Now suppose, it is working I do not know whether it is working or not. Do you know whether it is working or not? You try to steal something the next day you will know

where there is working or not. Most probably it is not working. See, what happens if I put the p t z camera first thing is that, I need to keep the data for x amount of hours. Suppose I keep my p t z camera on from night 8(o) clock to morning 5(o) clock, I do not think that people keep it on all the period lets us keep it.

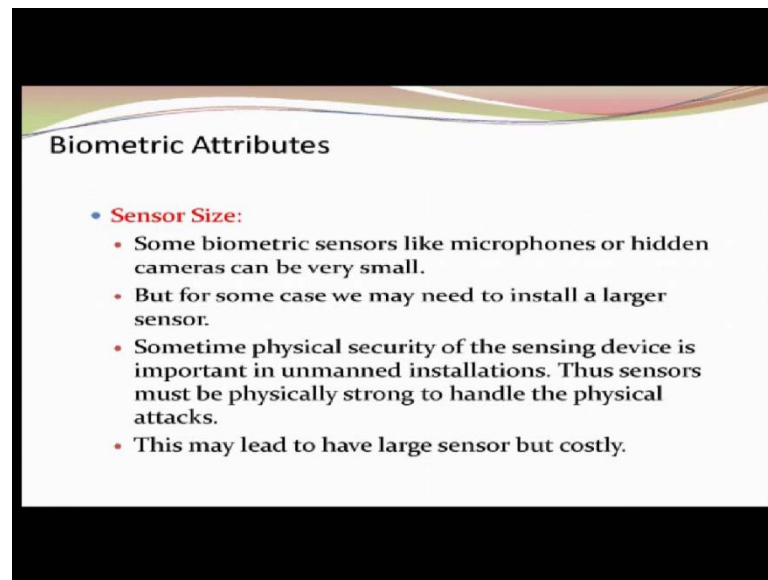
Now the volume of data you will be storing is huge. Suppose, I assume that, I have a system any change in the scene then my system clicks and it starts recording. Because, I cannot record it all the time then, there is a data will be huge. Only thing is that whenever there is a change in the frame I start recording till again it becomes the static one. Then also that volume of data will be huge; huge means I do not know how to handle this information. And in reality, if you see the data quality will be very poor and it is not easy to analyze those data.

Say for example, recently we got one data, it is been taken from the c c t v. And, it was for the 3 persons were riding on a motor cycle with gun and another things the gun is visible to 3 persons sitting on the motor cycle also visible, speed of the motor cycle is also visible or you can easily determine because I know the distance. I know the other information(s) that, there are some people looking at them those are also there.

But, I need to get the face which is very difficult even though they could detect the 3 persons but face getting itself is a very difficult thing, because you know rule is that in the motor cycle you have to wear the helmet; the helmets are there and on that helmets there is a glass cover.

So everything is gone it is a useless informations for me. So, that and that is why contact lens sensor you have to understand where you are going to use it. And, then only it will useful for you.

(Refer Slide Time: 13:16)



The slide is titled "Biometric Attributes" and features a decorative header with wavy lines in shades of green, yellow, and red. Below the title, there is a section titled "Sensor Size:" followed by a bulleted list of four points.

- **Sensor Size:**
 - Some biometric sensors like microphones or hidden cameras can be very small.
 - But for some case we may need to install a larger sensor.
 - Sometime physical security of the sensing device is important in unmanned installations. Thus sensors must be physically strong to handle the physical attacks.
 - This may lead to have large sensor but costly.

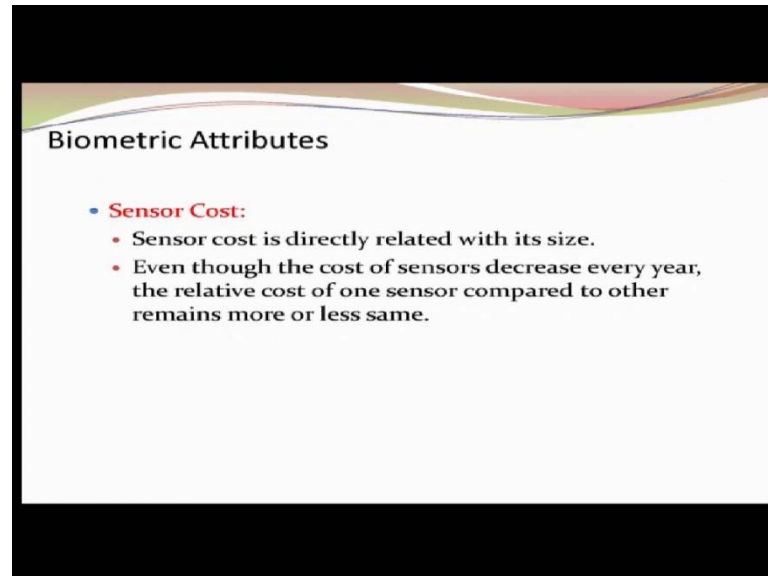
Now the sensor size is also another parameter. See suppose, I want to get information(s) or something from you over a table. Then, I do not need a bigger sensor to show it publicly that I want to take something information(s) from you. Instead of that I will be taking the hidden camera and I will be sitting and discussing with you so sensor time is very small. Now, if the sensor size is small obviously you will be getting the small information, resolution will be poor, there is a limitation on it.

And, if we need the larger sample sensor, sometimes it is required that I need a very good resolution and good coverage of the my system biometrics information. Of course, in that case you need a larger one; say for example, I want to get the palm print information(s) I need the larger sensor.

Say I want to get the 4 slab data. So, I need the larger informations but if I need only single finger print then I do not need the 4 slab size sensor, I need a very small size. And also suppose I put the larger sensor because say p t z camera I put fro surveillance and you know cost of the p t z camera is up to 2 lakhs rupees. So, it is a very costlier installation and what I can do? If I know that there is a p t z camera because intruder will be always knowing that, whether they exist some such type of things. So, I like to create some problem there. So I need to put some secured environment. So, that it is not physically destroyed, see I cannot put a gun man there to keep each p t z camera in safe condition.

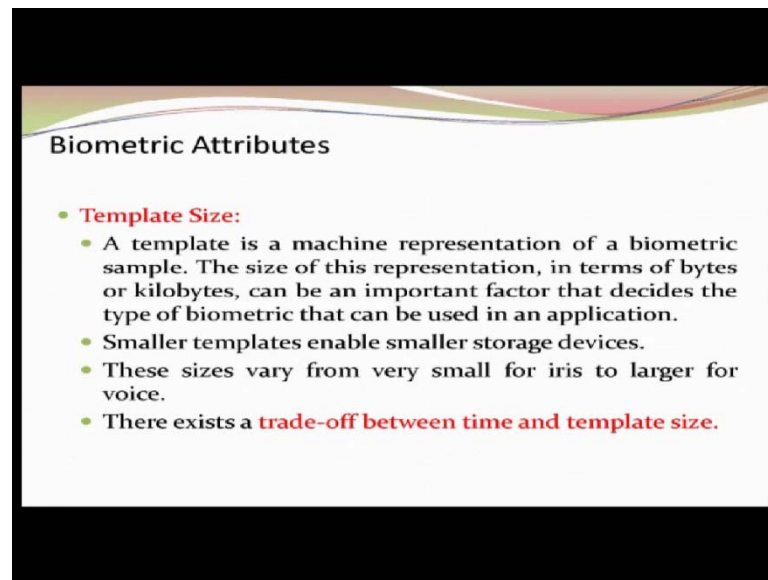
What I will do? I will make a iron frame, inside I will be putting my things all those things will be coming in between.

(Refer Slide Time: 15:54)



So, security of the physical security of my larger sensor is also an important parameter. And as a result the cost of the sensor becomes high. Now, the sensor cost is dependent on the size of the sensor. The smaller size sensor the cost is less, larger size is costly. Now, this is again one thing remember the physical cost is going down of each sensor that is true. But you know this not true for only one sensor, all type of sensors their physical cost is going down. So, relative change cost change is not that much change there is no change in with respect to the relative cost, agreed? So, that is also important parameters.

(Refer Slide Time: 16:45)



The slide is titled "Biometric Attributes" and features a decorative wavy line at the top. It contains a bulleted list under the heading "Template Size".

- **Template Size:**
 - A template is a machine representation of a biometric sample. The size of this representation, in terms of bytes or kilobytes, can be an important factor that decides the type of biometric that can be used in an application.
 - Smaller templates enable smaller storage devices.
 - These sizes vary from very small for iris to larger for voice.
 - There exists a **trade-off between time and template size.**

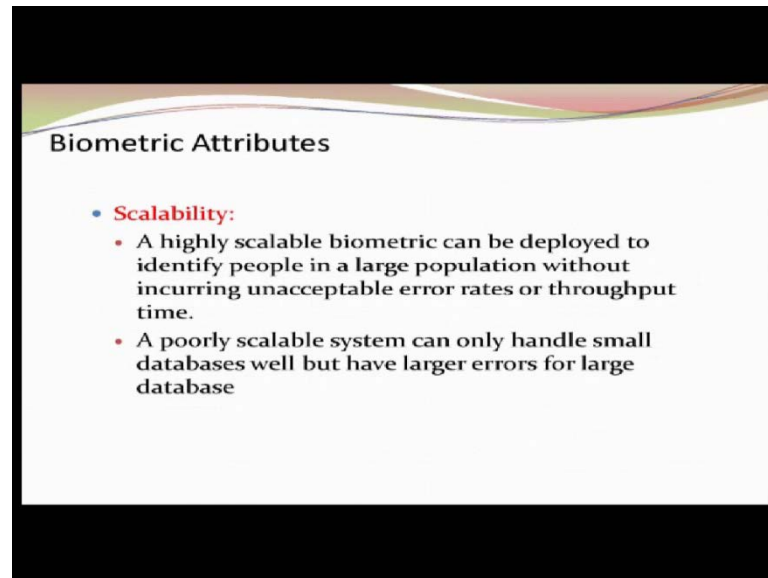
Templates size; you know smaller the template, better is that you need a smaller portion. You know what is template? Template is nothing but the features you are extracting from your biometric characteristics. Now, these features if the number is very less, then storage will be less, if length of the template is large, storage will be more. Now suppose, you have your smart card right in that smart card you have some chips, what is the size of the chips? 32 K or may be 16 K I do not think it is 64 K.

So in the 32 K you want to put your finger print information(s) how many fingers information(s) you can keep? How many minutiae points you can keep? Because minutiae points is nothing but your x y and theta and all of them each of them is of 4 bytes information(s).

So, to represent 1 minutiae point you need 12 bytes. So, how many minutiae points you can keep besides your name roll number and another things? So smaller the size of your template, it takes a smaller area and of course, it creates more problem for you, because you will not be able to store more number of vector features and as a result there is a chance of error. And smaller size is that you know Iris when we will be discussing you will find that this is nothing but it can represent using the bit vectors, so one bit one bit and so on.

So Iris even though it looks a bigger size but the size is very small compared to voice; because voice you need the features from the some a to b length of your speech. So, there exist a trade off between the time and the temperate size.

(Refer Slide Time: 18:58)



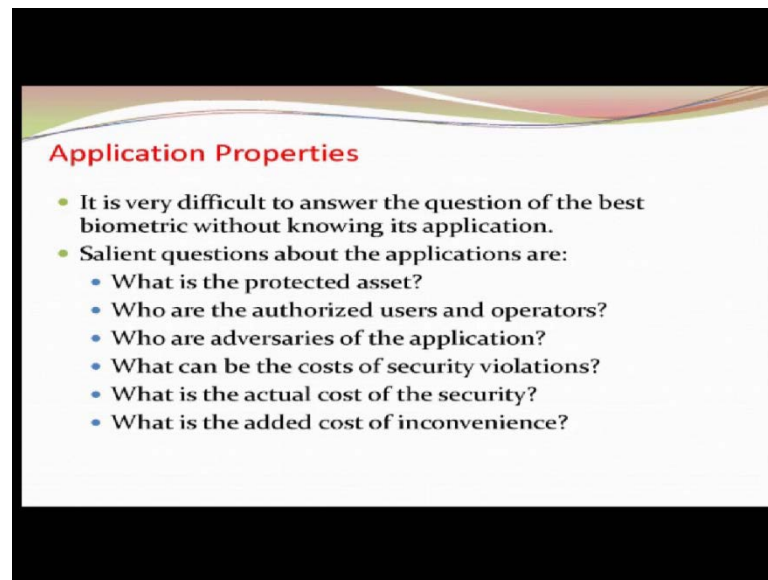
Biometric Attributes

- **Scalability:**
 - A highly scalable biometric can be deployed to identify people in a large population without incurring unacceptable error rates or throughput time.
 - A poorly scalable system can only handle small databases well but have larger errors for large database

Scalability is another parameter what you have to keep it in mind. What about algorithm or system you design? And obviously, you will not be designing that system in the field, you will be designing in the lab environment; in the lab environment database size is small; small means very small compared to the real life scenario. And in the lab environment you will be determining your $f_{a,r}$ and $f_{r,r}$ and also equal error rate and then you will be claiming that my system has this accuracy.

Now, once you tends for this thing into the field database size is huge. It must be scalable, you must be able to run that one under that condition. Not only that, you must ensure that your $f_{r,r}$ and $f_{a,r}$ they are same as you claimed at the time of selling your product. So, that is the scalability party you have to keep it in mind. A poorly scalable system is that it was very well in the lab but when I take it in the field it starts creating all sorts of problem.

(Refer Slide Time: 20:19)



Application Properties

- It is very difficult to answer the question of the best biometric without knowing its application.
- Salient questions about the applications are:
 - What is the protected asset?
 - Who are the authorized users and operators?
 - Who are adversaries of the application?
 - What can be the costs of security violations?
 - What is the actual cost of the security?
 - What is the added cost of inconvenience?

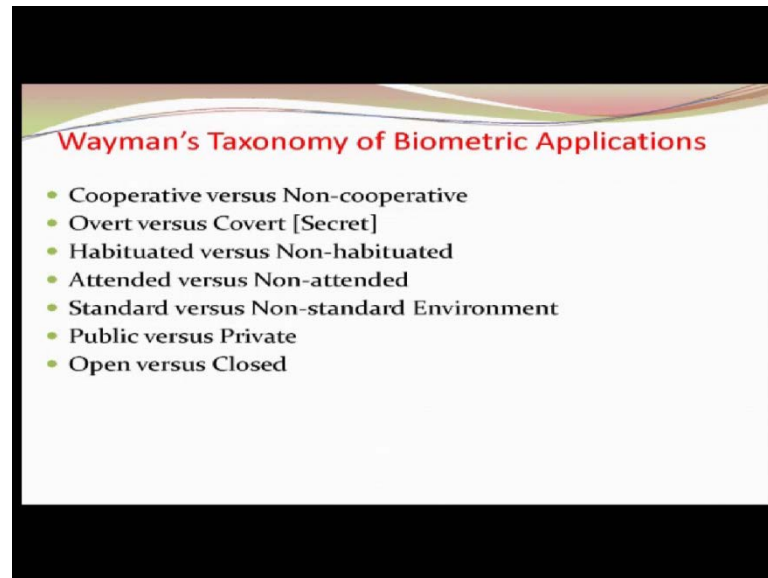
So, you understood that these are the issues you have to keep in mind while accepting a biometric system. But it is very difficult to answer the question which one is the best system. In order to understand that one you have to in order to use that one you have to explain yourself or you have to understand what is the application of your system? And some of the question you ask to the users.

One is that what is the protected asset? What for you want to use your biometric system? Why do you need such a system? That what is the asset? That you have to understand who will be authorized users and operators? Who will be coming into that or using that system? And who will be managing the whole environment? Who are the adversaries of applications that is who will be getting the benefits from this system? Now, benefit can be positive way can be negative way.

The negative way means, that if something goes wrong then I am in problem. Or, if something goes wrong then I may be benefitted I will get extra money for that. So, both the case you have to understand, because, you have to monitor them also. What can be the cost of the security violations? If by any means there is security breach, then what happens? How much loss you will be incurring? That is required to know, what is the actual cost of the security? Now, you will be doing deploying some biometric system now what will be the actual cost, because that is that should be if that cost is very high, because this cost is dependent on this cost.

So, you have to understand that which one and how to manipulate this one and what is the added cost of inconvenience, if you start doing that false rejection rate is high then inconvenience will be increasing what is that cost?

(Refer Slide Time: 22:38)



Now Wayman's taxonomy of biometric applications are based on these parameters. First you understand whether you like to implement a system which you use cooperative basis or non cooperative. That means is it expected that users will be **will be** giving his biometrics informations as and when required happily, whether they will cooperate with you to give his data.

Say for example, I ask that in order to draw the money from the bank, you have to give your biometrics data. You will be always happy, let me give my biometric data so that I can get my money so my money will be safe otherwise. But if I tell that **that** if you prove that you are the person then I will take 100 rupees from you. Then, in that case you will not be cooperating. You do not like to cooperate because I have to, if by any means it is matched with the biometrics data then, I have to pay 100 rupees so, I will not be interested.

So the cooperative verses non cooperative one is issue. Then, overt verses covert; overt is that I know that you are collecting data so, I will be little serious. If I tell you that I am collecting your photographs you will be serious, you will be putting some talcum powder on your face and another thing because somebody is taking your photographs. And

another one is that no without your knowledge I am collecting your photographs that is the covert. So, you have to understand these two also which one you want. Habituated verses non habituated; what it tells that signature suppose, if you sign on your checkbook you are habituated to sign it and that you know if I see your signature 10 signatures.

You have signed at different instant of times; you will find they are almost similar in nature. Now if I give you that no **no** signature on the paper I am not accepting you have to sign digitally, there is a digital pad and digital pen you sign on it, where while you are signing it is not possible for you to see what you are signing. Only it is showing in the display board so, display board is showing you that what you are signing and in the pad you are signing it. So, you are not habituated with this type of environment because we are habituated with that whenever **whenever** I am signing on a paper I see what I am signing. So, as a result what happens? You will find difficulty to sign on the digital pad; you are not habituated with this environment.

Same is the case with the finger print. If I tell you to give your finger print you can give it happily and you know that this is very simple you just put it on that so, it does not the need much here. But if I take that one in the village area they will come after cleaning all this thing, then they want to put it sometimes will put the finger little below the sensor some of them will put above the sensor all those things will come in between.

So they are not habituated. So, you have to that what is my subject whether they will be able to give me this informations. Attended verse non-attended; where are you going to use this system? Do you want to put somebody to monitor there, whether he is giving the data correctly or not or it is sufficient for me that I want to put a p t z camera and I am capturing the data.

So attended verses non attended issue you have to sort out. Standard verses non standard environment: what it means? That is it under lab environment or it will be in the open field? If it is in the open field, then you have to understand that issues of atmosphere is coming then, your sensor must be such that must be one that which can take care minus 5 degree or minus 7 degree to plus 50 degree, because your sensor should be deployable to every places under this condition.

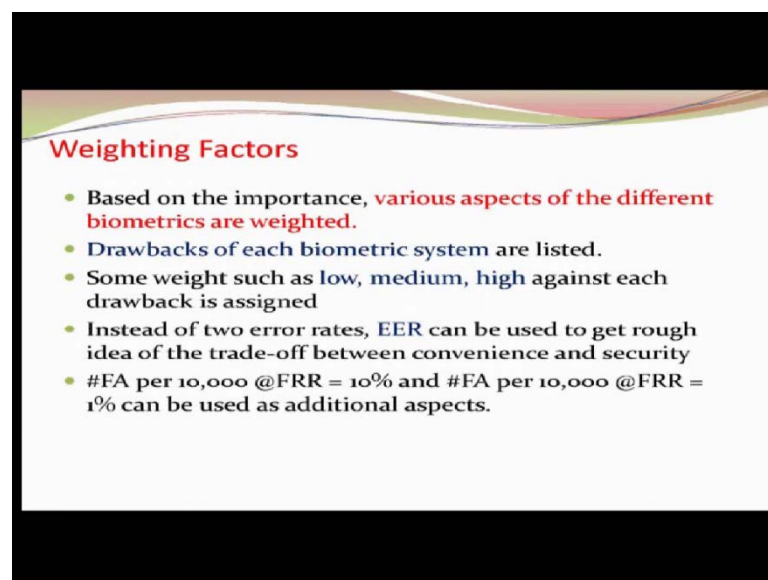
Similarly, humidity will be a factor all those issues will be coming so, you have to understand that one also. And then public verses private: are you going to use it

publically or in the private on this room itself only because that system will be different. And open verses closed: open verses closed means that database whatever you are considering is it open or it is closed? What is open? Open means that, in the database if I have n number of peoples biometrics informations the person whoever will be coming he will be one of them is your closed database. And, the person who is coming he may be one of them or may not be in that database list that is open.

Say for example, I get a dead body whose face is there and I got the dead body inside the campus. Now, is he a person in the database? It is an open database because, he may be in my (()) or he may not be there. But if I assume that in my classroom sitting people that database is closed this is closed because you are in my classroom attendance list.

So, if you understand if you ask these questions to the employers or to the customer you will understand that which are the biometric suitable for this activity. Once you know then you will find the only few will be there. Now, the cost for acceptance error rates and other issues you put it obviously you will be able to determine which one is your best choice.

(Refer Slide Time: 29:43)



Weighting Factors

- Based on the importance, **various aspects of the different biometrics are weighted.**
- Drawbacks of each biometric system are listed.
- Some weight such as low, medium, high against each drawback is assigned
- Instead of two error rates, EER can be used to get rough idea of the trade-off between convenience and security
- #FA per 10,000 @FRR = 10% and #FA per 10,000 @FRR = 1% can be used as additional aspects.

Now, there are several factors we have introduced and all this factors has certain values. Based on the importance of the system biometric system which you like to deploy in an institute various aspects of the different biometrics are weighted, because there will be many few of them. Now, you have to give that each of the certain aspects, you have to

weight them, that weight will be used to determine that which biometrics you want to use it. So each biometrics has certain drawbacks, you understand drawbacks clearly and note down that these are the drawbacks I have for this biometrics state for Iris these are the drawbacks that you note down.

And against each drawback, you put some weights; say low medium high or one high lying between 0 to 10 you put some weights. Further instead of using 2 error rates, because 2 error rates will tell you about the convenience and the security. If you remember in the last class you have defined what is security and convenience. These two error rates will help you to drive this one. Here, you can use equal error rate of the training set, the number of false acceptance per 10000 at the false rejection rate of 10 percent, this can be one parameter another one is number of false acceptance rate per 10000 at false rejection rate of 1percent can be used additional aspects. So it is here I have written forcibly 10 percent you can increase decrease whatever it is but once you define that one.

(Refer Slide Time: 31:40)

Weight	Physical Access	ATM Use
Intrinsic Properties		
• Required Cooperation	Low	Medium
• Social Stigma	Medium	High
• Population Missing	Low	High
Sampling Properties		
• Inconvenience	Medium	High
• Acquisition Time	High	Medium
• Failure to Enroll	Medium	High
• Failure to Acquire	Medium	High
1:1 Matching Properties		
• # FA per 10K (@FRR = 10%)	Medium	Medium
• # FA per 10K (@FRR = 1%)	Medium	High
• Template Size	Low	High
Technology Properties		
• Installation Cost	Medium	High
• Computational Run Cost	Medium	High
• Cost per Match	Low	Medium

Now, let us assume that one is the physical access that I want to enter into my classroom, another one is that ATM users. Intrinsic properties you need required cooperation or not. So these are all some random value I have put, some low required cooperation is low in the case of physical access because I want to keep the p t z camera and your cooperation is not required but ATM use you need medium.

Social Stigma: Social Stigma means that, suppose I tell you that you have to give your finger prints sometimes society does not accept that one, they feel I know how to sign why shall I give my finger prints. Say recently, in the t v add is coming: a lady is standing in the queue and then the supervisor is telling put your finger print and she is telling no **no** I know how to sign. So, the Social Stigma is important thing and then population is missing in the case of physical access, I know this people will be coming, missing population will be 0 because these are the people.

But in the case of ATM coverage is not 100 percent very few people are using the A T M. So ATM users population missing is high, sampling property inconvenience if false rejection is there how much inconvenience will be there? ATM users will have heavy because if I want to withdraw money I will not be able to get the money. And then obviously that is the reason why I put high.

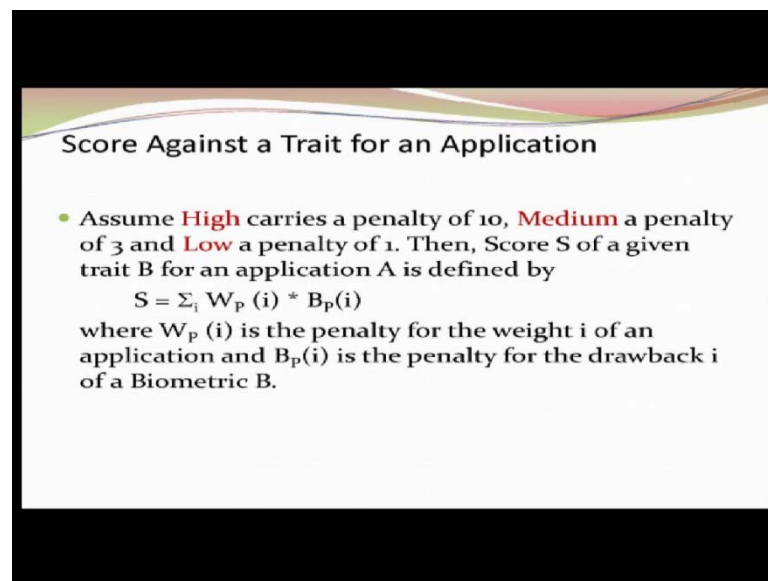
Acquisition time: how much time it takes to give you the data failure to enrollment rate and failure to acquire rate, these are also I have put there some number 1 is to 1 matching properties number of false acceptance per 10000 with FRR 10 percent we have written something and false acceptance rate per 10000 for the FRR 1 percent is that and template size is low and high we have written. Technologic properties installation cost is what you have to see then, computational run cost and cost per match. These are the parameters we consider for both the things.

(Refer Slide Time: 34:34)

Trait Properties			
Biometric Drawbacks	Finger	Face	Iris
Intrinsic Properties			
• Required Cooperation	High	Low	Medium
• Social Stigma	High	Low	Medium
• Population Missing	Low	Medium	Low
Sampling Properties			
• Inconvenience	Low	Low	Medium
• Acquisition Time	Low	Low	Medium
• Failure to Enroll	Medium	Low	High
• Failure to Acquire	Medium	Medium	Medium
1:1 Matching Properties			
• # FA per 10K (@FRR = 10%)	0.1	10	0.001
• # FA per 10K (@FRR = 1%)	10	1000	0.1
• Template Size	500	1000	250
Technology Properties			
• Installation Cost	Low	Low	Medium
• Computational Run Cost	Low	Low	Medium
• Cost per Match	Medium	Low	Low

Now, if I see with respect to the traits one so, corresponding to the traits we obtain these are the drawbacks and finger, face and iris we have obtained. These values we have written. Now these are no, now you could obtain for both the case that for the requirement wise, what are the issues I have noted down. For the biometrics characteristics also we have noted down what are the drawbacks and these values we have put. Now, which biometrics will be suitable to know that, what I want to do that I put that I replace these high low medium by some value say 1 3 10.

(Refer Slide Time: 35:25)



Score Against a Trait for an Application

- Assume **High** carries a penalty of 10, **Medium** a penalty of 3 and **Low** a penalty of 1. Then, Score S of a given trait B for an application A is defined by
$$S = \sum_i W_p(i) * B_p(i)$$
where $W_p(i)$ is the penalty for the weight i of an application and $B_p(i)$ is the penalty for the drawback i of a Biometric B.

If I know these 1 3 10 or some values, then score I can obtain the submission over $W_p(i)$ into $B_p(i)$, the weight for the institute and weight for the biometrics state.

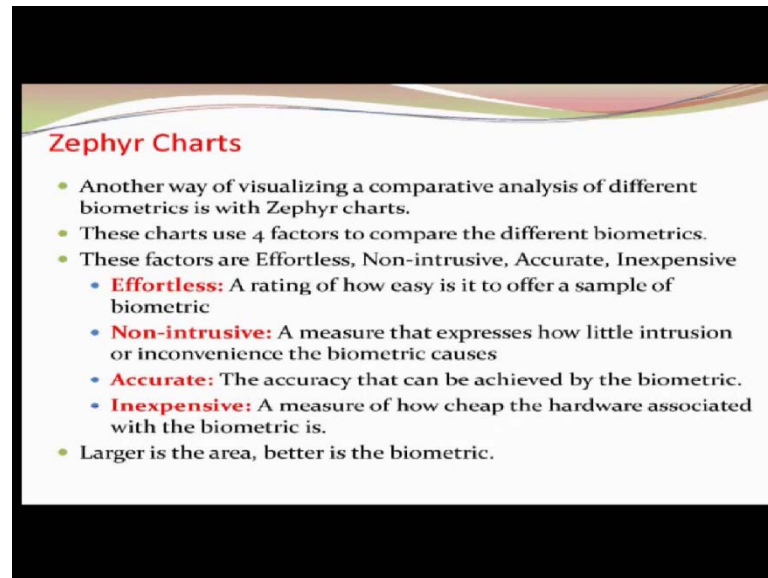
(Refer Slide Time: 35:39)

Score Computation- An Example		
Score	Physical Access	Fingerprint
Intrinsic Properties		
• Required Cooperation	Low (1)	(10) High
• Social Stigma	Medium (3)	(10) High
• Population Missing	Low (1)	(1) Low
Sampling Properties		
• Inconvenience	Medium (3)	(1) Low
• Acquisition Time	High (10)	(1) Low
• Failure to Enroll	Medium (3)	(3) Medium
• Failure to Acquire	Medium (3)	(3) Medium
Matching Properties		
• # FA per 10K (@FRR = 10%)	Medium (3)	(1) 0.1
• # FA per 10K (@FRR = 1%)	Medium (3)	(10) 10
• Template Size	Low (1)	(5) 500
Technology Properties		
• Installation Cost	Medium (3)	(1) Low
• Computational Run Cost	Medium (3)	(1) Low
• Cost per Match	Low (1)	(3) Medium
SCORE = 110		

So if I put that weight, suppose physical access is this and finger print is that one and the weights I have put and I got the total scores is 110. Similarly, you can obtain the other traits and based on that which is having the higher score you tell, higher score you tell that, it is not acceptable to you, lower lowest one you want for your use.

Am I right? is it ok? So, using that means you need to know that industrial drawbacks why I need this thing how much cooperation I need all those thing you find out, and at the same time you obtain the each biometric states corresponding drawback values then, you collide them or fuse them or we obtain the weighted average or weighted sum to obtain the score, the minimum score value you take for your system

(Refer Slide Time: 36:39)



Zephyr Charts

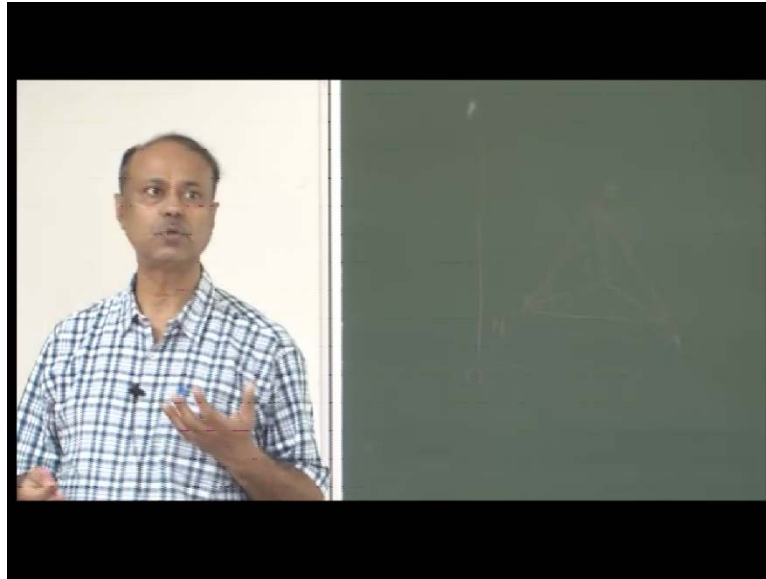
- Another way of visualizing a comparative analysis of different biometrics is with Zephyr charts.
- These charts use 4 factors to compare the different biometrics.
- These factors are Effortless, Non-intrusive, Accurate, Inexpensive
 - **Effortless:** A rating of how easy is it to offer a sample of biometric
 - **Non-intrusive:** A measure that expresses how little intrusion or inconvenience the biometric causes
 - **Accurate:** The accuracy that can be achieved by the biometric.
 - **Inexpensive:** A measure of how cheap the hardware associated with the biometric is.
- Larger is the area, better is the biometric.

The other one, other way of also measuring that which system is better that is known as Zephyr **Zephyr** Charts. Now, this Zephyr Charts gives you or is measured based on these 4 factors. How much effort is required in your biometric system? That can be obtained by from the training that iris takes this much effort, finger print takes this much effort; you can tell it is very much effort is required 0 effort is required you can easily determine that one, that is important parameters; non intrusive that is it creating the inconvenience to people? How much is, it a very inconvenience every time you are rejecting a genuine person or no most of the time.

Some parameters you can find out from there. How much accuracy the system gives and is it inexpensive? How much expensive it is? These 4 parameters, **parameters** you can easily explain in the scale of 0 to 10 yes possible; Possible yes or no? Because how much effort I give you the 4 5 **4 5** biometrics scan sensors and used by 100 peoples they write down in the scale of 0 to 10 for each of them, this is the effort I need full effort I do not need much effort. So 0 to 10 scale and then you make average and standard you can obtain this one.

Inconvenience, how many times it is making the failure to false rejection rate that you can find out, accuracy you can easily find out and then cost is also important.

(Refer Slide Time: 38:54)



So if I know these things so can I have this is a, will it be say it is first one is effortless error is non intrusive accuracy and another one is expensive. So, can I have this, three dimensional figure on a three dimensional structure; that one, is the expensive parameter 0 to 1 scale. If I have this side is, 0 to 1, 0 to 1, 0 to 1. So, I have a 3 dimensional figure. Now this three dimensional figure if I can obtain that what is the total area volume I can obtain that so that if the volume is less and then you tell that this is the better biometrics for you.

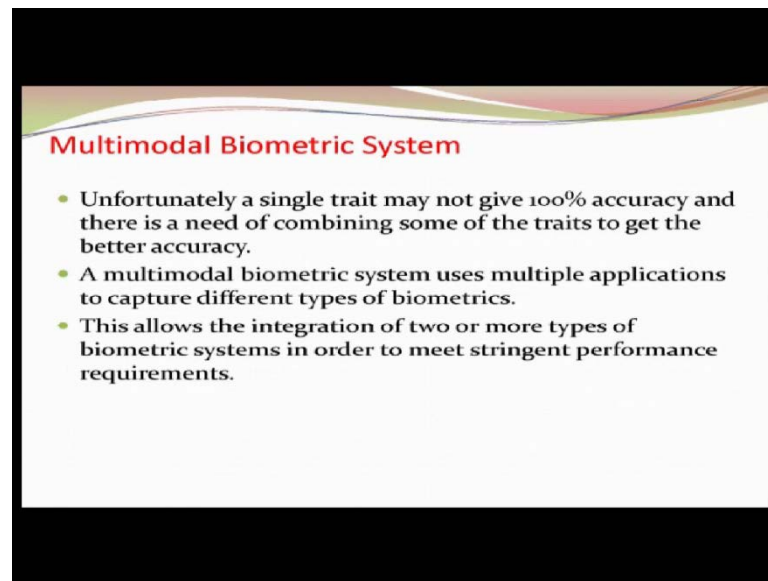
(Refer Slide Time: 40:05)

Zephyr Chart

Factor	High	Medium	Low	Lowest
Effortless	Iris	Face	Finger	Voice
Non-intrusive	Iris	Voice	Face	Finger
Accurate	Iris	Finger	Face	Voice
Inexpensive	Voice	Finger	Face	Iris

This is the one example which I have put it.

(Refer Slide Time: 40:10)



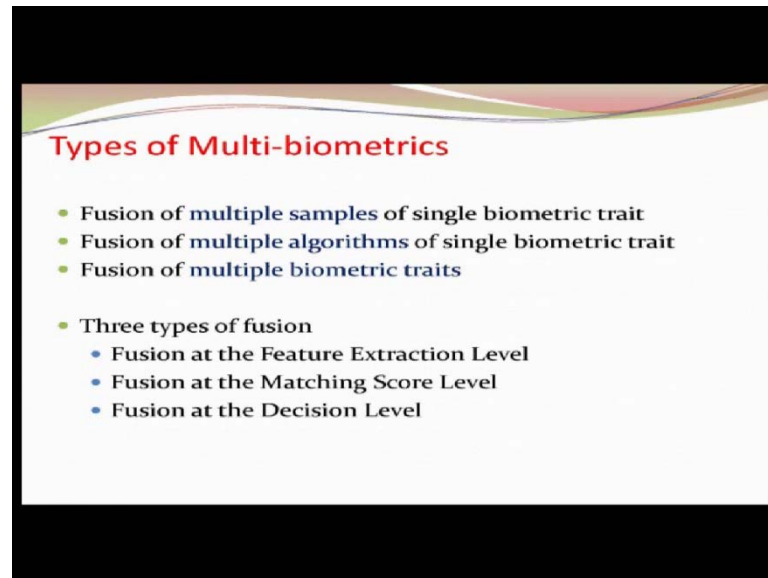
Now, the term is coming Multimodal Biometric System. By now you realize, so single biometrics you know that you have the false acceptance rate and false rejection rate; it will be there it cannot be 0. You can make one 0, then other will go up. So accuracy cannot be 100 percent and another thing I can tell you that, from suppose I have a system which has 85 percent accuracy, there is a still chance to improve you system to achieve may be 90 percent up to 90 percent. But, suppose I have a system of 98 percent accuracy to improve by 0.5 percent there will be very **very** difficult.

So, that is the bad part of the pattern recognition system, say improving by very small amount for the higher percent accuracy things is very difficult. But everybody wants that a system I want to deploy which is 100 percent accurate. So, this 100 percent accuracy cannot **cannot** be achievable by a single biometrics state. So what we can think, that can I use the different biometrics traits and you fuse these results to improve your accuracy. You combine this say it may so happen that if I assume that his biometric information or finger print information and he has given also the face information and if one of them is matched, he is allowed to enter.

So, obviously the accuracy will go up. So, that indicates that the integration of two or more biometrics is required, to get the better accuracy. But still it is not proved that multimodal will give the better result than the single biometric. Now better means what?

Better, means I have the money more biometrics state more money I have to pay. So, those issues are also there because cost verses cost is also important parameter cost verses the amount of security is required.

(Refer Slide Time: 42:27)



Now, what are the different types of bio multi biometrics? One thing can be that I collect multiple samples of the same biometrics trait and then you fuse them. For example, I take the 2 iris data and I use both the results combine it or I take the 10 fingers and I match 10 fingers instead of single fingers and then I should get the better results.

What should be my fusion strategy? That is later on but I combine the results, by some methods. Another one is that, I have the different algorithms of face recognitions and each algorithm gives me some results I combine them and give the results that, is also possible. And another one is that, I use multiple biometric traits that means, I take the face, finger print, iris or others and you fuse them. So, these are the three ways you can think to design your multimodal biometric systems.

Now, how to fuse them? Here, I have not mention the fourth one because fourth one we are not interested. First let us talk about the fourth one, then I get the sensor data this sensor data is an image form and another sensor data say I got a finger print data it is in the form of image another one is say, face data it is also image form I combine them, I make one image.

So, finger print having say, 100 cross 20 and another one is face is having, 180 cross 300 and I combine these two I get volume, that is the lowest level fusion image fusion which we are not interested.

So, first one is that feature extension level fusion that means that I got the features from one biometric trait and say ear is there ear biometrics traits I got the features and also face biometrics trait and I got the features I combine them, I concrete them that is possible or I take the fusion of some of the methods to combine these two that is possible feature level. Then another one is that fusion at the matching score level; what it means? That you will be matching your finger print with another finger print you got a score and similarly, you matched iris against another iris you will be getting another matching score.

Now, remember that one matching score may give you similarity match the other one may give you the dissimilarity match or one matching score is lying between 0 to x another matching score maybe giving you the range minus y to z. So, both of them you have to normalize it and you make it in one platform and then you fuse it. How you will be fusing that is different but some method you will be adding this two matching score to get one matching score and then using the threshold value you except or reject that decision you can make.

Third one is that, decision level that suppose, I want finger biometric state gives you the indication that you are accepted the other one is telling also accepted 100 percent you are accepted. Similarly, one is rejected and other also is rejected you, then it is 100 percent rejected. The another case is, one telling accepted and another one is, telling rejected that is there is a need to decide. So the fusion at decision level so these are the ways you can fuse them.