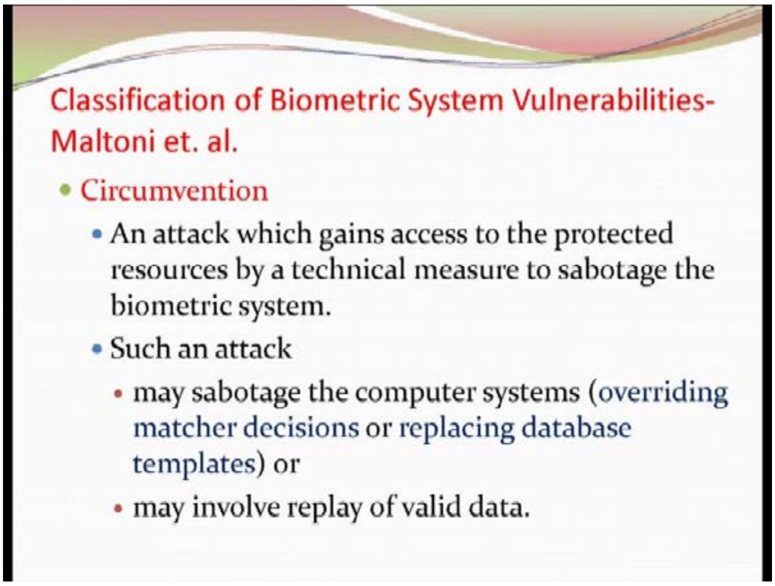
Biometrics
Prof. Phalguni Gupta
Department of Science and Engineering
Indian Institute of Technology, Kanpur

Lecture No. # 16

We are discussing about the biometrics security, that you have the system and what the are weak points in your system that has to understood carefully and this is the classification of biometrics system vulnerabilities. And Maltoni is the person, who wrote this, who have just previously I told the way man's classification.

(Refer Slide Time: 00:30)



Classification of Biometric System Vulnerabilities- Maltoni et. al.

- Circumvention
  - An attack which gains access to the protected resources by a technical measure to sabotage the biometric system.
  - Such an attack
    - may sabotage the computer systems (overriding matcher decisions or replacing database templates) or
    - may involve replay of valid data.

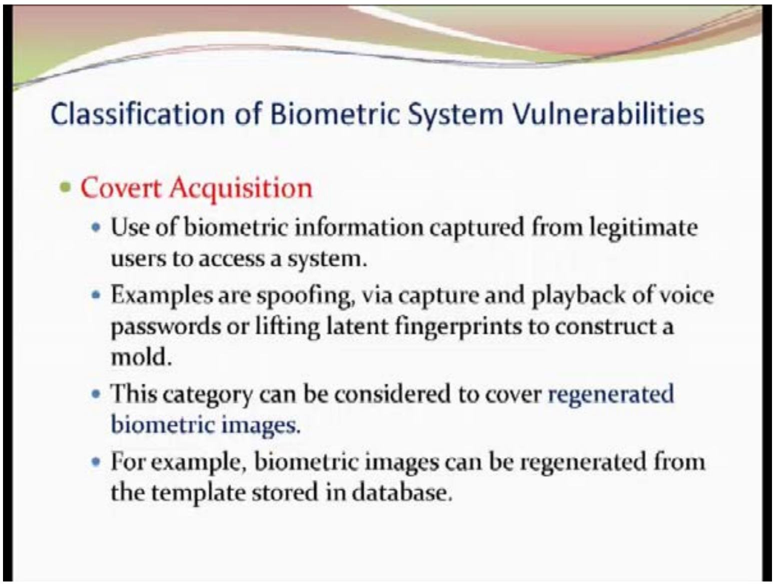
Here it is Maltoni's classification. And the first point is the circumvention. What it tells, that it is an attack that gains access to the system by some technical method to sabotage your biometric system. So, this attack can be the sabotage the computer system. What it means, that you want to override that matcher.

That matcher tells fails but you did some manipulation, you make it. No, it is accept. Now, this first one is that you may there may you can sabotage the whole system, the computer system itself, what it means that the hardware you will be sabotaging. You are sabotaging the matching algorithm or feature extraction algorithms.

There you do some manipulation that a person, who is supposed to get yes, you can make it no or no you can convert into yes. Another one is that, whatever irrespective of feature you get or matching, you just replay the old data. Suppose, I want that he should be fake, so I got the feature from the concerned persons but instead of using that feature you use your own available features. So, that he will be fail.

Or you want to make him pass always. So, whatever feature you extract from the image but you put such one that which is always making it accept, that means his old data you are old features you put it and make it accept. So, these are the two ways you can attack the system. This is circumvention. Then covert acquisitions and you know that covert acquisitions means that it is not that your involvement is required to provide your data and that is the use of biometric information captured from legitimate used to access the system. So, I am the genuine person, I captured the data and I you have captured my data that information I will be using for my purpose.

(Refer Slide Time: 02:55)



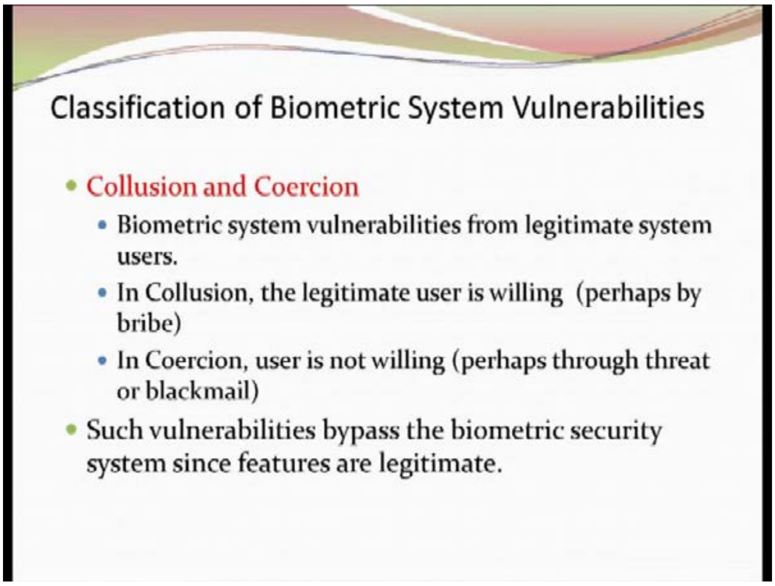
Classification of Biometric System Vulnerabilities

- Covert Acquisition
  - Use of biometric information captured from legitimate users to access a system.
  - Examples are spoofing, via capture and playback of voice passwords or lifting latent fingerprints to construct a mold.
  - This category can be considered to cover regenerated biometric images.
  - For example, biometric images can be regenerated from the template stored in database.

So, examples are spoofing, that is why I capture and playback of the voice what signature, whatever is there that you will be paying back or there is a somewhere you gain your fingerprint, I have taken the photograph of it and then I extract the features, I used it for further purpose. This category can be considered to cover the regenerated biometrics template.

So, what happens that you once you get this latent fingerprint; now from the fingerprint, you have to regenerate the features; similarly, from the features you have to regenerate the fingerprint also. So, even though one can think that the from the feature I may not be able to regenerate my fingerprint but the people, who have started working on it, that is it possible that given features, can I get back the original image. So, that work is going on. So, the regeneration is an important parameter here.

(Refer Slide Time: 04:01)



Classification of Biometric System Vulnerabilities

- Collusion and Coercion
  - Biometric system vulnerabilities from legitimate system users.
  - In Collusion, the legitimate user is willing (perhaps by bribe)
  - In Coercion, user is not willing (perhaps through threat or blackmail)
- Such vulnerabilities bypass the biometric security system since features are legitimate.

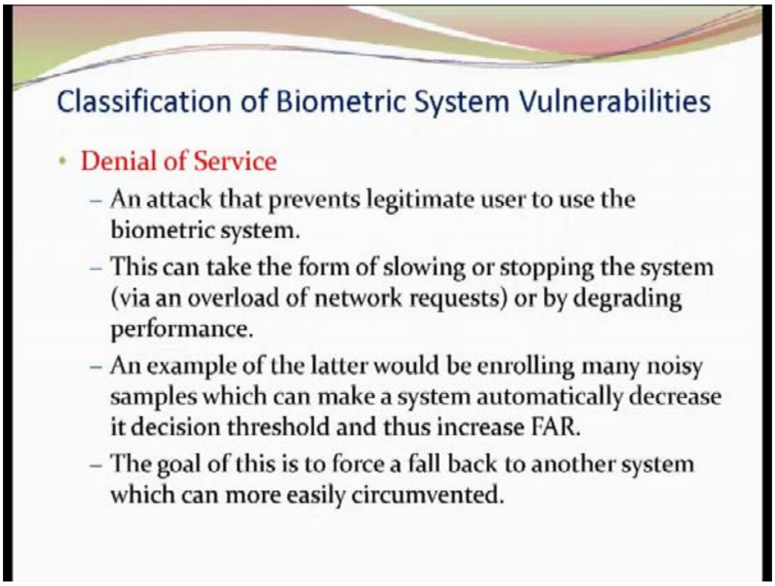
Collusion and coercion. This is one thing remember that this occurs from the legitimate user only. Sometimes, what happens, that the legitimate user also wants to break the system. So, what are the possible cases?

In the case of collusion, he is willing to get it rejected. I want to provide my data in such way that I get rejected. That is possible case that if I get rejected, then others will be benefited. So, what happens that I tell you I tell you that you get rejected, then I will pay you x amount of money. So, obviously you will tell ok. Why I, there is no problem if I get the x x amount of money. I am ready to sacrifice my thing.

So, this is another under collusion. The collisions it here, it is the reverse one, that he is not ready to give the biometrics, not the he is not willing to sacrifice his stand. Yes, I will give the data to get it accepted. But here I am giving you threatening or the I am blackmailing, you that you have to get accepted, so that you I get benefit from it.

So, these are two conditions and in that case, there is no way; you can because both of the in both the cases, user is legitimate, genuine user. So, it will be through. So, you cannot detect that attack. Now, the denial of services is also another type of problem here we are facing, that this attack prevents a genuine user to use the system.

(Refer Slide Time: 06:07)



Classification of Biometric System Vulnerabilities

- Denial of Service
  - An attack that prevents legitimate user to use the biometric system.
  - This can take the form of slowing or stopping the system (via an overload of network requests) or by degrading performance.
  - An example of the latter would be enrolling many noisy samples which can make a system automatically decrease it decision threshold and thus increase FAR.
  - The goal of this is to force a fall back to another system which can more easily circumvented.

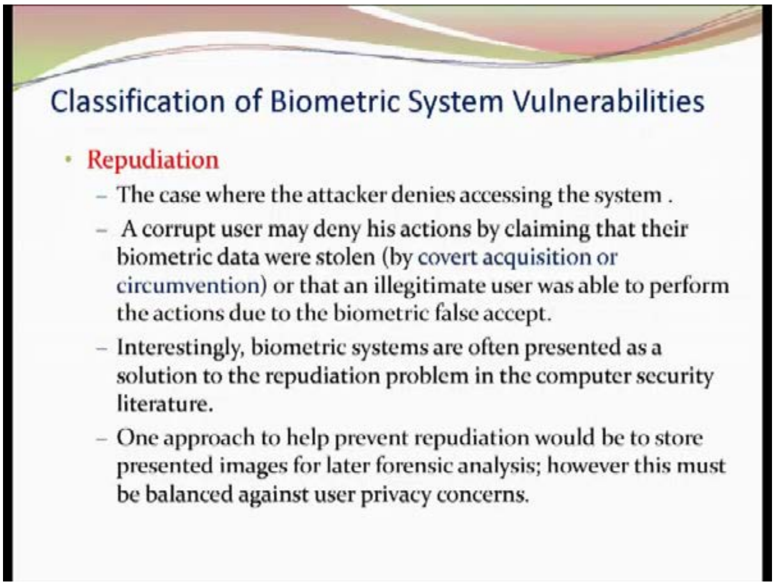
Now, how can it be possible? This can be in the form of that you you can make the system stop or or slowing down your network or that you reduce the performance of the system. So, what how can reduce the performance or degrade the performance. The degradation can be done, say once you extract the features, you can put you can put a lot of noise on it and once you have put the noise, there is a possibility that there will be too many false feature points and as a result, that genuine person will be rejected.

So, he will be denied from the service. Or another way could be that you have put a lot of load under your network, the system gets slow. Now, the legitimate user he comes; he wants to prove himself but because of the slowing down system, it is taking huge amount of time. So, you the person will tell no because generally, what we put that we put some time constraint that if it beyond this period, you tell that rejected.

So, you will be thrown out and again you will be denied. So, generally in such cases what happens, that user or the industry will tell that, oh this system is no good because it is giving you lot of problems. So, let us change it. So, change it.

And once you change it that means that the concept of concept of handshaking will come in between, that compromising with the other one that in circumvention and other factors will be introduced in that case. It will be easy for.

(Refer Slide Time: 08:01)



Classification of Biometric System Vulnerabilities

- Repudiation
  - The case where the attacker denies accessing the system .
  - A corrupt user may deny his actions by claiming that their biometric data were stolen (by covert acquisition or circumvention) or that an illegitimate user was able to perform the actions due to the biometric false accept.
  - Interestingly, biometric systems are often presented as a solution to the repudiation problem in the computer security literature.
  - One approach to help prevent repudiation would be to store presented images for later forensic analysis; however this must be balanced against user privacy concerns.

Repudiation is one thing that you cannot deny that you have done this thing. So, a legitimate user has come and he has given the data and he should not tell that no I have not done. But there are some places, where you may find that I have given the data and I am claiming that I have not given the data, my data has been stolen. My voice has been stolen by somebody.

This you get very frequently wherever forensic science problem comes, that you will find that it is not my voice. It is somebody who has copied my voice. And this is one thing remember, this is openly available; the voice is available, fingerprint is available. You have given some place in fingerprint, I have copied it and I have extracted the features and I have used.

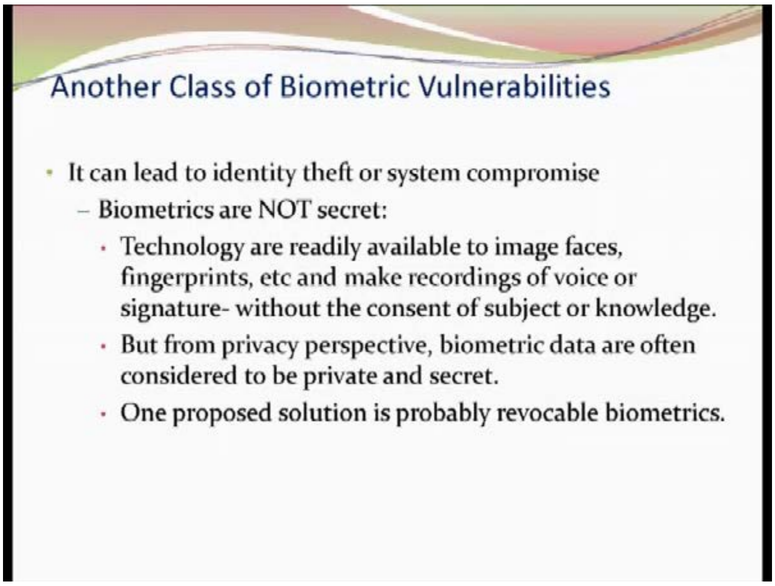
So, you can tell that my biometrics information is stolen. Or by some means I could get your, say biometrics features and I have enter into your system and that is also possible. But if the same thing, if you keep in mind that we use biometric system to avoid the repudiations.

That means, what we are telling that to the protocol that tells that you cannot deny that you have not done these things. That is possible through biometrics. That is the outlay but here at the same time on the first part, what we are telling that no. Sometimes it may so happen that. Generally, a user may tell no, I have not done; somebody has stolen my voice, somebody has stolen my fingerprint. So, I am not responsible for that. This may happen.

So, this two contradicts each other and as a result, one solution could be like this, that whatever action you do, whatever image you give I store it. Keep it for future purpose and if you disclaim or if you claim that no, it is not my I have not given the data, then I can extract the image and I can prove that yes, it is you have given this data, at this situation.

But one issue is coming up. In that case that image becomes in public domain because you are not the person, who will be analyzing. It is another group, who will be analyzing this, that whether you have given the data or at that time or so or not. So, image becomes in public (()) in privacy may be and shown here.

(Refer Slide Time: 10:46)



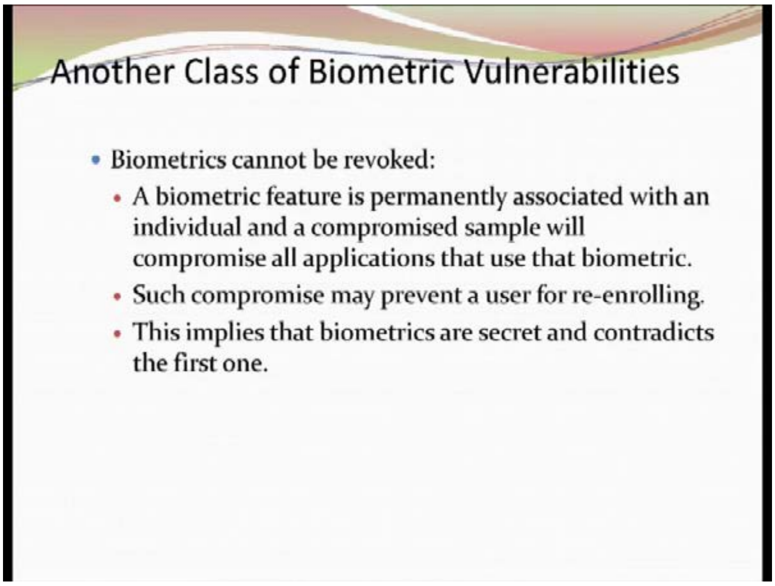
Another Class of Biometric Vulnerabilities

- It can lead to identity theft or system compromise
  - Biometrics are NOT secret:
    - Technology are readily available to image faces, fingerprints, etc and make recordings of voice or signature- without the consent of subject or knowledge.
    - But from privacy perspective, biometric data are often considered to be private and secret.
    - One proposed solution is probably revocable biometrics.

It can lead to identity theft or system compromise. Biometrics are not secret. So, the technology exists to get your photographs, whether if with your permission or without your permission; to get your fingerprint with your permission or without your permission, this technology exists and once it is there, so you cannot claim. That the it is a secret.

So, from the privacy point of view, you always tell that biometrics data I have to retain it, it is a secret, it should not be sharable and all those things. So, there is a contradiction between the two statements.

(Refer Slide Time: 11:32)



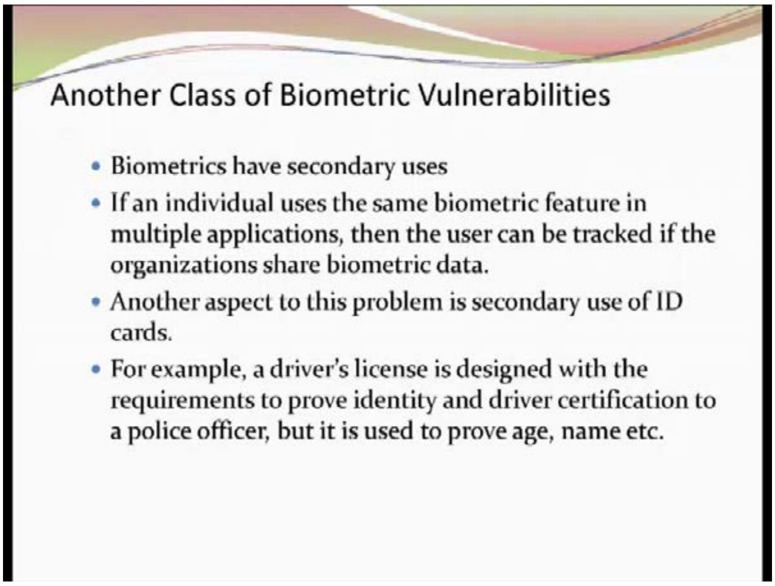
Another Class of Biometric Vulnerabilities

- Biometrics cannot be revoked:
  - A biometric feature is permanently associated with an individual and a compromised sample will compromise all applications that use that biometric.
  - Such compromise may prevent a user for re-enrolling.
  - This implies that biometrics are secret and contradicts the first one.

So, one may one can think that the data whatever you are getting, biometrics says that can I make it secret or revoked. So, this is also possible, that you move the data in such a way, that it becomes the encrypted. You cannot be, no one can get it back. Now, this is also possible. Now let us understand, if it is the possible thing, one and once you give the data and it is revoked. It is encrypted by some else and now, that you have a compromise system and that is allowing the people. So, he will not be, you are not thinking that you will be able to do it. What you can do that, you if in case there is a problem, you just change your fingerprint data or your biometrics data and again, you start using.

But here again the problem is that you cannot change it because that compromise system also change (()). So, that will be a big problem for you. So that, this is not a correct threshold. This is a, that replace the biometrics system. Biometrics data is secret; itself is a contradictory statement. You cannot think that it is a secret all the time.

(Refer Slide Time: 12:56)



Another Class of Biometric Vulnerabilities

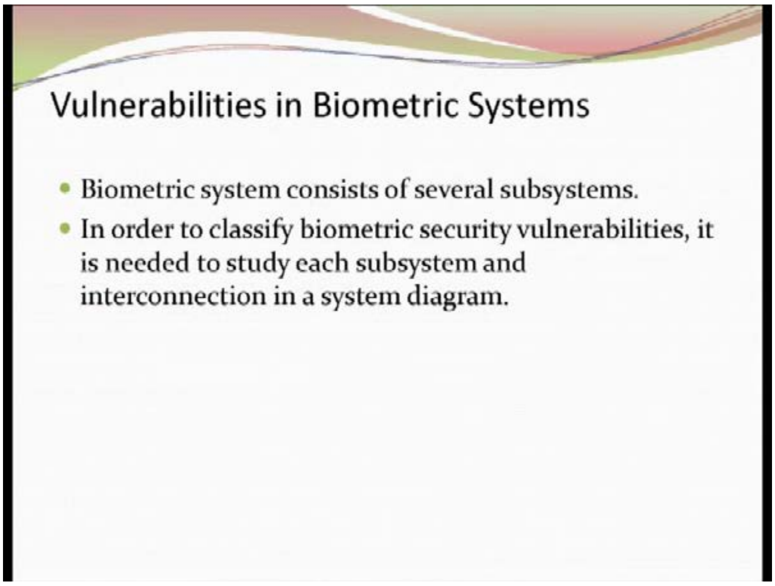
- Biometrics have secondary uses
- If an individual uses the same biometric feature in multiple applications, then the user can be tracked if the organizations share biometric data.
- Another aspect to this problem is secondary use of ID cards.
- For example, a driver's license is designed with the requirements to prove identity and driver certification to a police officer, but it is used to prove age, name etc.

Or you can manipulate through some encryption thing. No, in that sometimes, you know the biometrics data we use for secondary purpose also. Suppose, an individual has given the biometrics data for multiple purposes.

Now, if the organizations the different organizations share that information because I have given my fingerprint, why shall I give every time? I have given my fingerprint, face data and other data to different thing and I want to use same data for multiple purposes.

That means what? The organizations will be sharing the data. So, if it is that, then user can be tracked using by that but at the same time, how can you tell the privacy is retained and another aspect in the case of secondary users, the driving license is designed with the requirement of to prove the identity and driver's certification to a police officer, but it is used to prove the name and age also. So, this is also multiple use of your, example of multiple use of same data. So, usually you have used it for what? For driving purposes but it has been used for other purposes also.

(Refer Slide Time: 14:22)

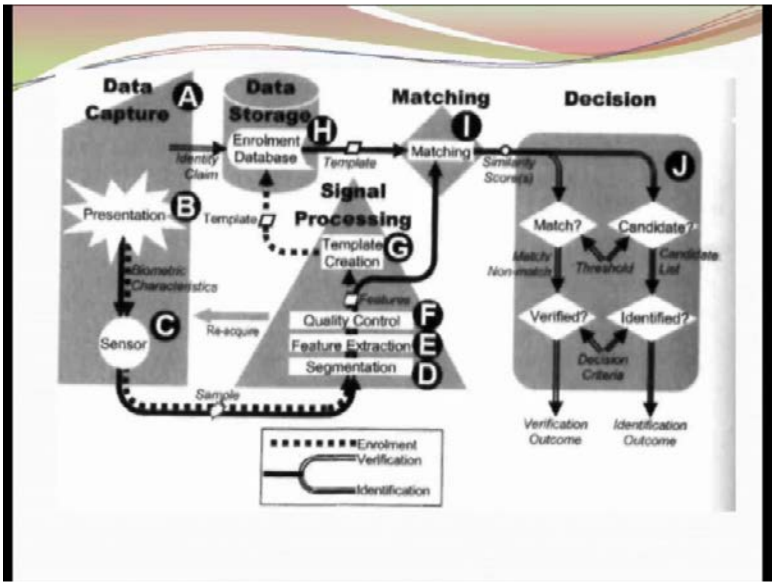


Vulnerabilities in Biometric Systems

- Biometric system consists of several subsystems.
- In order to classify biometric security vulnerabilities, it is needed to study each subsystem and interconnection in a system diagram.

Now, let us think about, you know that biometric system consists of several subsystems. Agreed and now, each subsystem is connected with another subsystem. So, vulnerability can occur in at any stage, in the subsystem or in another in the league or connection between the two, at the time also it may occur.

(Refer Slide Time: 14:49)



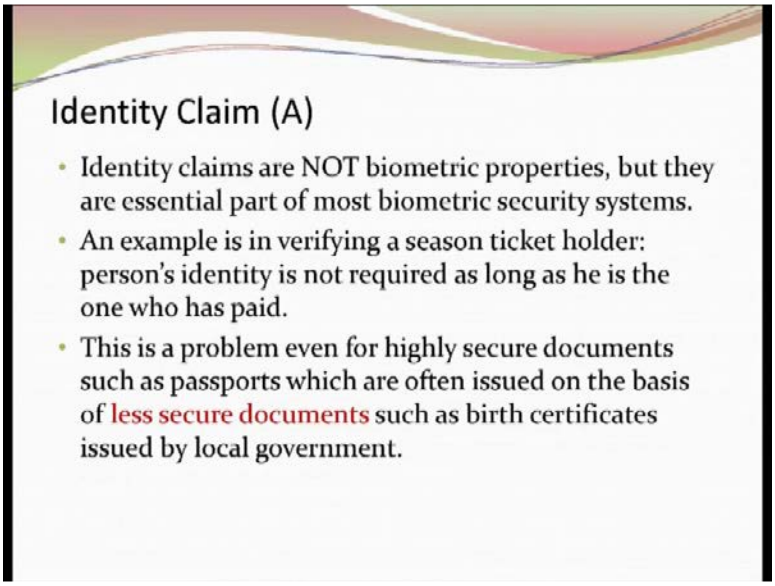
For example, if you see this diagram, you come and you give your data. You project the data that I have come and presented data. So, what it means, that I have come and I have you have to say, as you have given your data in the Adhar card, what you did? You have gone there, then you have given your high school certificate or address proof and so so, many things.

So, you tell that yes I want the Adhar card. I have this this data. They have also given the set of papers you have to bring. So, they check, yes you are eligible to provide your data, then you provide the data through sensor. Once the sensor gets the data, then you will be extracting the features, segment first segment, then feature extractions, then quality control. If quality fails, you have to do again.

If it is a successful, now you will be generating the template and once, it is a first time template generate, so you have to go to the enrolment place, that means the database, data storage and if it is for verification, then it will go for matching. So, it will match, from this take to data match and then, he take verification or identification. Based on this, they will take the decision.

Now, you observe that wherever I have written a b c d e f g h, this all of them are the point of vulnerability. The vulnerability can occur may occur here and may occur here and may occur here, here, here. Template generation type then, data storage type matching and so on. So, you have to understand how it is happening. So, let us first think about identity claim. What is the vulnerability there?

(Refer Slide Time: 16:35)



Identity Claim (A)

- Identity claims are NOT biometric properties, but they are essential part of most biometric security systems.
- An example is in verifying a season ticket holder: person's identity is not required as long as he is the one who has paid.
- This is a problem even for highly secure documents such as passports which are often issued on the basis of less secure documents such as birth certificates issued by local government.

Identity claim is not a biometric system, that you have come with some papers and you want to prove that I have come, I want to. So, but this is also indirectly essential part of your biometrics system development. Even though, your that the paper is not useful but it is essential. For example, here in the simple case simple case that you have a you know season match is there, season ticket is there and you are claiming every day. You go to see the movie or to see the game. If you have the ticket, they will not ask.

And again, if you even though they write that it is not transferable but if you give the season tickets to somebody else, he also will enter because he does not mean anything because he has paid money for so many tickets and he is sharing, is not a big issue. Now, think about the highly secured documents case, the passport.

You have passport, yes or no? Who has a, everybody has passport. Now, what? No, he does not have the passport. You do not require. You require. You have a passport? You do not have, you do not want. What for? So, you want to go abroad. No, there are several reasons, why I need passport. You know; yes or no? Is it only for going abroad? What identity is there?

But what is identity, there is no identification mark there. They verify what. That somebody else has checked your candidature and I am honoring that candidature. Not beyond that you can draw anything. So, same is the case here also. If you see that I want to prepare make a passport, they tell you that you give your address verification thing. So, generally we give the address verification and maybe ration card. You have a ration card? No. or if Remember one thing, ration card is the most important thing in life.

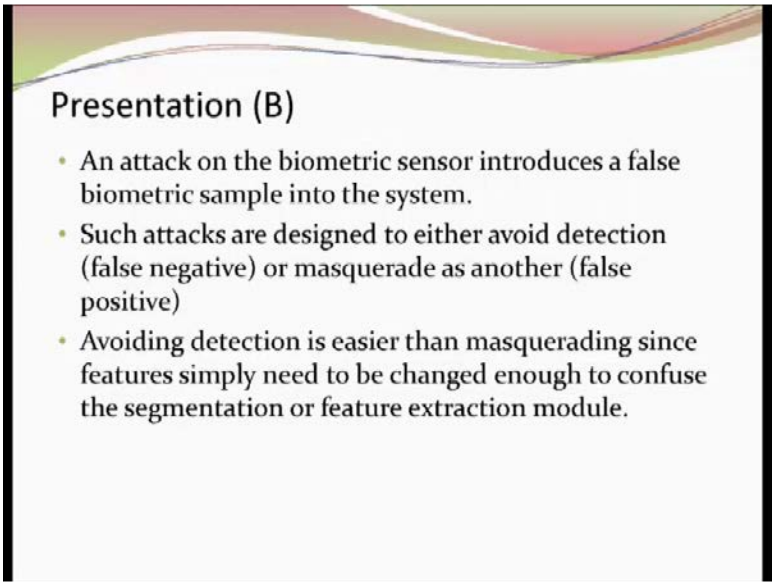
If you do not have the ration card, you will not get the gas connection. Now, to get the gas connection, you need the ration card. So, tell me how to solve this problem, I do not know. So, you know you have to do some manipulation here and then, to get one ration card first. Once, you get the ration card, then you will get the gas connection. If you get the gas connection, then you get the address proof, because gas has been delivered to your house.

Ration will not be delivered to your house. You have to go there to bring the ration. So, who is going; where, nobody knows. But gas connection depends on but to get the gas connection, you need the ration card. So, you have gone to that you have to fill the form, where you have to show that address proof. So, generally people give the ration card address and once, you give the ration card address, who verifies the ration card. Nobody comes to verify.

Generally, I have not seen that anybody comes and checks you, whether this address is correct or not. Based on that, they give you. So, less you know secured system is giving you some authenticated thing to get the higher secured things. That is the thing. To get the passport you need the address and the address is the proof that you are getting from the ration card, which is lower level secured environment. Am I right?

So, this itself is a, when this passport you are going to use for further processing as you are telling. So, if it is based on the weak authentication system, then everything is gone. Now, the presentation is another one. Just you have come with the data that whatever data you are you are presenting in front of the sensor yourself and then, you have to tell I am this, I want want my authentication and or I want to enroll myself.

(Refer Slide Time: 21:08)



Presentation (B)

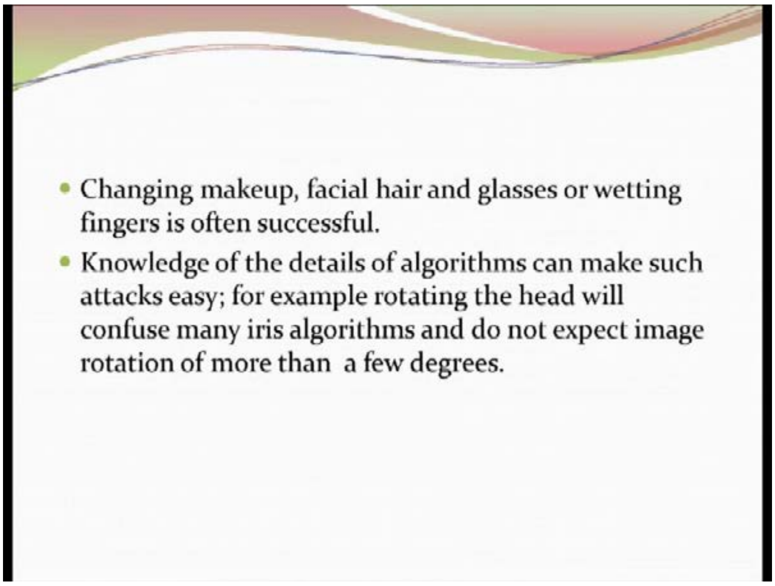
- An attack on the biometric sensor introduces a false biometric sample into the system.
- Such attacks are designed to either avoid detection (false negative) or masquerade as another (false positive)
- Avoiding detection is easier than masquerading since features simply need to be changed enough to confuse the segmentation or feature extraction module.

So, the same attack on the biometric sensor. This attack will introduce either the false biometric sample into the system. It is a false biometric sample into the system. Such attacks are designed to either avoid detection. So, you will be given the, so that you will not be able to detect. So, false negative or masquerade, as another that is false positive.

Now, that avoiding detection is much much easier problem compared to the masquerading. Because that in the case of avoiding detection, just say for in the case of fingerprint, I just cut my finger and I give that. So, you will not be able to because I have come with my fingerprint. There is no ambiguity. I have come with my fingerprint, I have brought my materials and now, I want to give the data. Whatever data, I will do with my fingerprint is cut. So, features will be different. Even though, your sensor is good.

But if I had to generate somebody else features on my fingerprint that is a more difficult problem. The simple problem is that I want to avoid my detection. So, I come with a some cap round fingerprint cap, I give the data, so wrong features will be extracted is very easy but the other one is difficult. That no, I want to prove myself not, I am not Phalguni Gupta, I am Saibul Islam, then his fingerprint I have to have is a difficult problem. So, presentation is one thing.

(Refer Slide Time: 22:49)

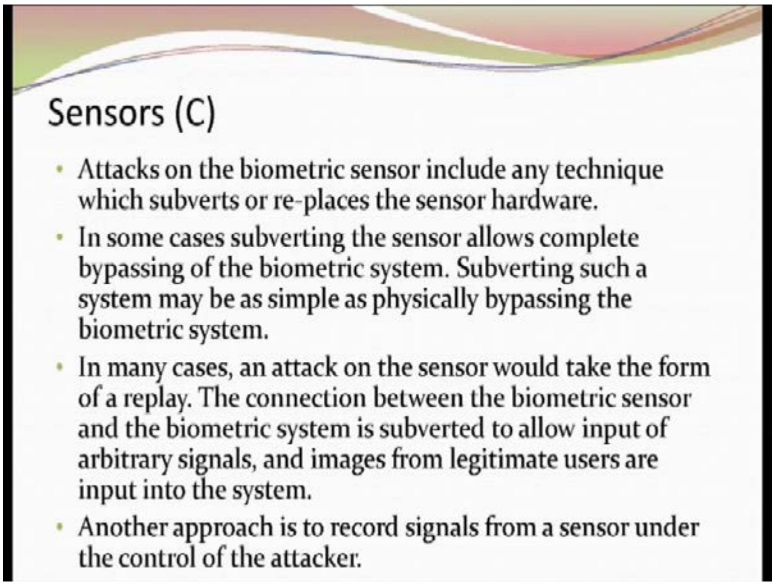


- Changing makeup, facial hair and glasses or wetting fingers is often successful.
- Knowledge of the details of algorithms can make such attacks easy; for example rotating the head will confuse many iris algorithms and do not expect image rotation of more than a few degrees.

So, the example is that you can in the case of direction problem avoid detection. You can put the makeup. You can put the moles here, you can put the beard or you can put some fingerprint cap or you can cut the fingerprint. These are all successful thing.

Now, if I know the algorithms in detail how features are getting extracted, then this attack is much easy. So, suppose I want to make the (()) of my system and I take the, I provide my iris data in the reverse order, that head is bottom and leg is up. In that case, my system will fail because my iris algorithm is works only for few degree rotations. So, these are the issues in front of your presentation.

(Refer Slide Time: 23:50)



Sensors (C)

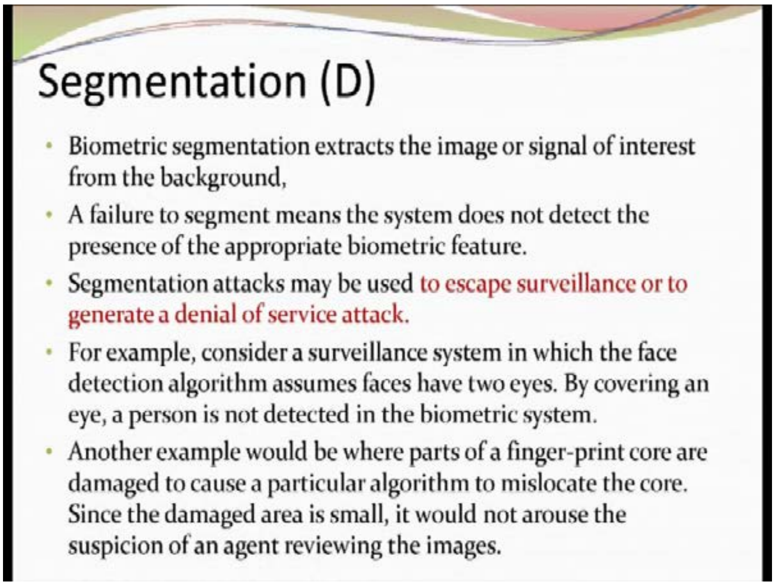
- Attacks on the biometric sensor include any technique which subverts or re-places the sensor hardware.
- In some cases subverting the sensor allows complete bypassing of the biometric system. Subverting such a system may be as simple as physically bypassing the biometric system.
- In many cases, an attack on the sensor would take the form of a replay. The connection between the biometric sensor and the biometric system is subverted to allow input of arbitrary signals, and images from legitimate users are input into the system.
- Another approach is to record signals from a sensor under the control of the attacker.

Now, sensors is also another place, where the attack can be possible. So, one way could be that you put the poor quality device, quality is always giving you the wrong, poor quality, poor quality, poor quality and you will become fed up and you will go, I will not use your system. Is it possible?

But in the same time, so in that case what happens that you can completely bypass the system. You can directly go to the operator that I am failing every time, so can you help me? So, he will use your his own thinking and the system will be broken. Some in some cases that what happens that whatever data you give, he replays a old; whatever store data is there, he transmit that one for future extraction.

So, I have given my image on the scanner and the scanner is not accept, even though he is showing you that he has accepted your image but he is transmitting not your image; somebody else image. Whatever he has in his cash, he is transmitting. So, that way also he can bypass the system and so, this is always under the control of attacker. So, the attacker decides that whose data has to be transmitted from the sensor.

(Refer Slide Time: 25:24)



Segmentation (D)

- Biometric segmentation extracts the image or signal of interest from the background.
- A failure to segment means the system does not detect the presence of the appropriate biometric feature.
- Segmentation attacks may be used to escape surveillance or to generate a denial of service attack.
- For example, consider a surveillance system in which the face detection algorithm assumes faces have two eyes. By covering an eye, a person is not detected in the biometric system.
- Another example would be where parts of a finger-print core are damaged to cause a particular algorithm to mislocate the core. Since the damaged area is small, it would not arouse the suspicion of an agent reviewing the images.

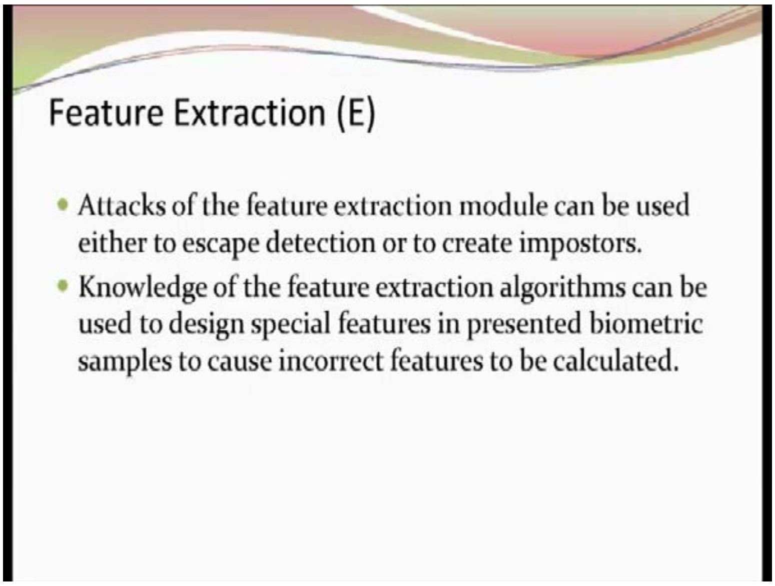
Now, sensor has transmitted the data. The data transfer means that image. Now, that at this image segment, you have to get the R O I. That image segmentation you have to do. This point also there is vulnerability. Where is the vulnerability, where the system has to detect the R O I. So, there may be some case, system is not able to detect the R O I. For example, I have used the surveillance camera to get your face photographs. You have given your face photograph, there is no problem. I system has collected your face.

Now, to get the to detect your face, I have used the two eye black part, that black portion of your eye or iris I have used to obtain your R O I. Now, suppose surveillance camera is attached such that your system is able to detect only one eye, either one way that you have closed one eye or system has collected the data such that the another eye is not visible. Then the system will not be able to detect his R O I.

Similarly, is the case with the; suppose, I use the core point in the fingerprint, there is a you check there is a centre point. That center point I use to detect my R O I but it is not essential. He is looking up whether there exists a centre point or not in his finger. May not be there but most of the people are having the centre point.

Centre point is the where you will find that all curvatures beyond that is going up. That is one point is known as centre point. Now, suppose there is a cut in the centre point, area is very small. So, it is difficult or it will be difficult for any system to obtain the R O I in that case. Because this algorithm works based on the core point.

(Refer Slide Time: 27:34)



Feature Extraction (E)

- Attacks of the feature extraction module can be used either to escape detection or to create impostors.
- Knowledge of the feature extraction algorithms can be used to design special features in presented biometric samples to cause incorrect features to be calculated.

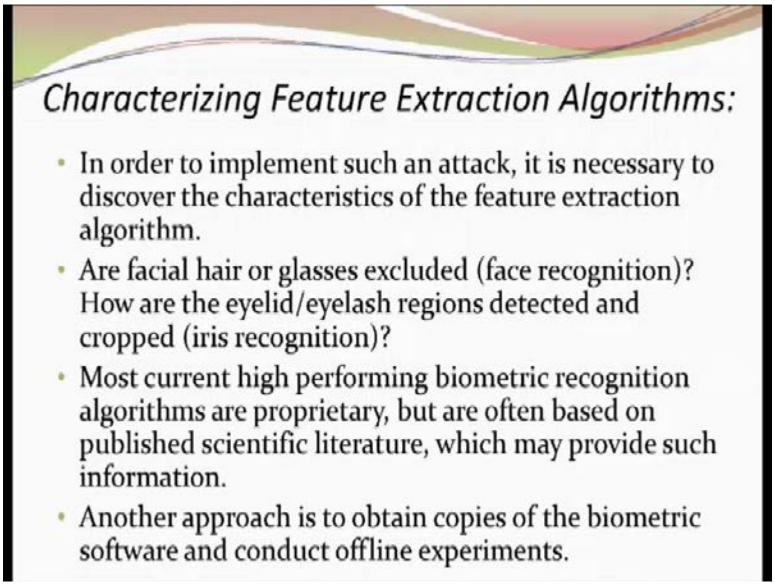
Next one is feature extraction level. Is it is it vulnerable? This module input is the R O I. Now, if it has passed through R O I, that means he has got some area of his fingerprint and from there you have to extract of his biometrics data and he has to extract some characteristics from there.

So, it can be used for both the cases. One is that I want that imposter should be in. That means forgery is allowed. That I want that his case should be forged or I want to see that he is not he is not allowed to enter into the system. In both the cases, that means that a genuine user will be rejected and imposter will be accepted, which are extraction level forgery or attack on this can work for both the cases.

Now but in order to in order to do that, you have to know what feature extraction algorithm he has used. Otherwise, you cannot manipulate or you cannot attack. So, the knowledge of the feature extraction algorithm is very useful in this case. So that, if you know that one, so you need to generate some special features. Say, I have the fingerprint minutiae points is the things I need to reject his case.

So, I have to introduce extra minutiae points and those minutiae points should not be the minutiae points whatever he is having, first one. Or second one is that I want to reduce some of his true minutiae points or I want to introduce some true minutiae points. So that, the candidate will be accepted, even though he is an imposter. In that case, he has to know the algorithm. Not only that, he has to know the persons or minutiae points, which has to be entered into the say forcibly.

(Refer Slide Time: 29:56)



Characterizing Feature Extraction Algorithms:

- In order to implement such an attack, it is necessary to discover the characteristics of the feature extraction algorithm.
- Are facial hair or glasses excluded (face recognition)? How are the eyelid/eyelash regions detected and cropped (iris recognition)?
- Most current high performing biometric recognition algorithms are proprietary, but are often based on published scientific literature, which may provide such information.
- Another approach is to obtain copies of the biometric software and conduct offline experiments.

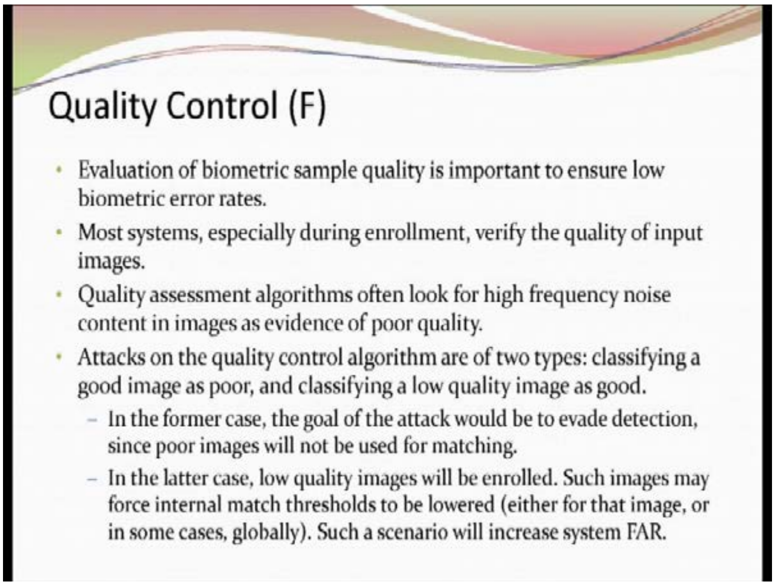
So, how to characterize extraction feature extraction algorithms? So, you as I told you earlier, you have to understand the algorithm carefully. See, in the case of face, you can think that I am designing a feature extraction algorithm for face. Here, you have to understand whether he is considering hair into hair into account or not.

If he is considering in his R O I hair is he in into account then, it is a different problem. Then he has to think that how to how to get the features, where your R O I is R O I contains hair also. Or in the case of iris, you can think that whether eyelid or eyelash regions are thrown out or not. There is some algorithm, where you will find that no; I have considered both eyelid and eyelash.

Some cases, what we have seen that I consider the eyelid and eyelash area. If it exist, that exists in the upper part of the iris. So, I do not consider, I take only the bottom part. Some area, we consider this eyelid or eyelash or eyelid as an occluded area, I do not consider. So, there are different ways one can think. So, you have to understand the all these cases, to introduce new features in the system. Most of these biometrics recognition algorithms are proprietary.

So, even though, you know this but they are proprietary system. Nobody will tell you what algorithm is used have been used to develop the system that means his proprietary. But unfortunately all these feature extraction algorithm is based on from the algorithms available in the literature. So, you have to understand the literature, algorithm available in the literatures and you have to find out what algorithm he has used, based on that you have to act on it. So, this is the about your feature level attack.

(Refer Slide Time: 32:12)



Quality Control (F)

- Evaluation of biometric sample quality is important to ensure low biometric error rates.
- Most systems, especially during enrollment, verify the quality of input images.
- Quality assessment algorithms often look for high frequency noise content in images as evidence of poor quality.
- Attacks on the quality control algorithm are of two types: classifying a good image as poor, and classifying a low quality image as good.
  - In the former case, the goal of the attack would be to evade detection, since poor images will not be used for matching.
  - In the latter case, low quality images will be enrolled. Such images may force internal match thresholds to be lowered (either for that image, or in some cases, globally). Such a scenario will increase system FAR.

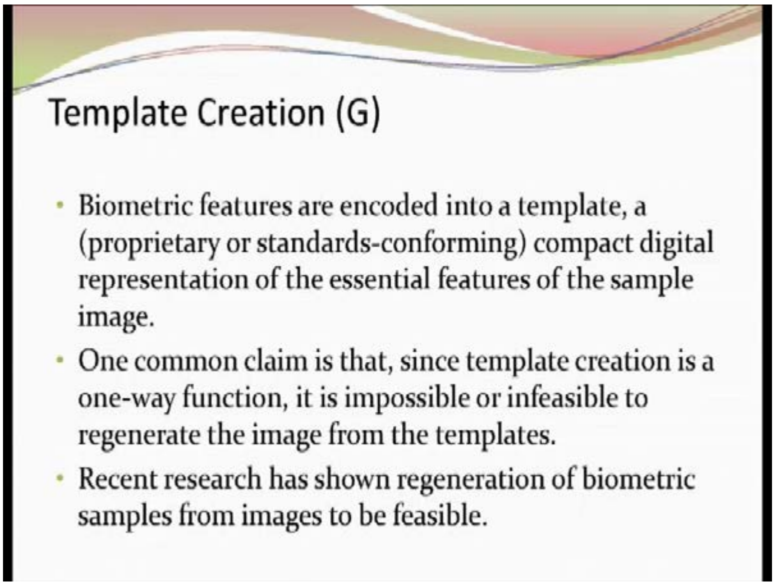
Quality control, where as I told you that once, I have extracted the features, you will be checking this quality and you will be telling that this quality is poor. If it is poor, then you will be throwing back, that telling that no you have to provide your data again. So, this is one point, where you know you can always reject a person or always accept a person.

Say, evaluation of biometrics sample quality is important to ensure the low biometrics rate and during enrollment, you verify always you have to verify because quality is poor because my aim, I am always expecting that my data in the database must be very good. So, you will be verifying and you remember one thing that, this is the factor way a quality you can always take care that is poor. Even is a poor quality data you will be telling no it is good.

If good quality data you are telling poor, then you are throwing him out from the enrollment. The person will be giving the data again and every time you will be telling that no, no it is not good and exceptionally make may be coming in between. Because he has not been able to provide his data. or Or it may so happen that you are falsely rejecting a person. If it is every time I am giving and you are quality is poor and ultimately, the concerned operator will tell okay, let us accept this data and then, system will throw him out. So, false acceptance, false rejection will be there and if you make the poor qualities very good, what happens?

That everybody's data will be accepted in a for the enrollment or for the verification of identifications and you will find that false acceptance rate will be high. So, the this is once one vulnerability, that quality control at that level it may occur.

(Refer Slide Time: 34:24)



Template Creation (G)

- Biometric features are encoded into a template, a (proprietary or standards-conforming) compact digital representation of the essential features of the sample image.
- One common claim is that, since template creation is a one-way function, it is impossible or infeasible to regenerate the image from the templates.
- Recent research has shown regeneration of biometric samples from images to be feasible.

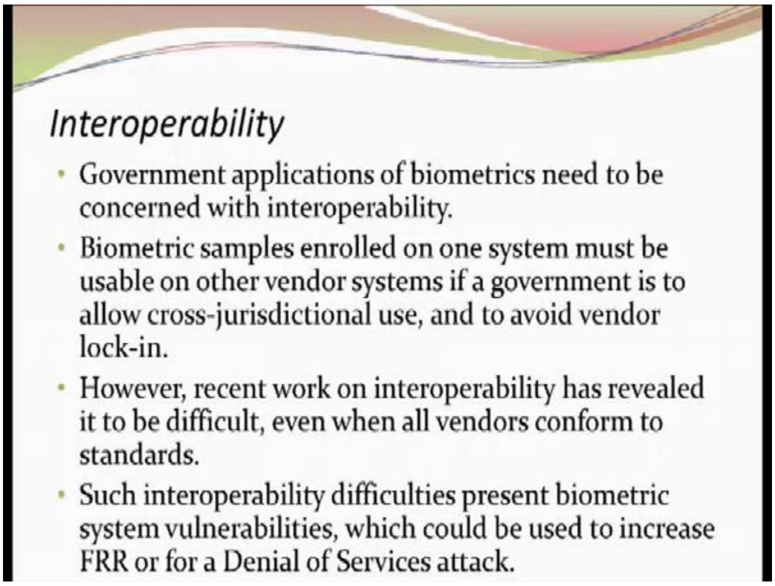
Now, once quality is passed, then you will be generating the template and template is a feature vector, your it may be it is assumed to be unique and if I can manage to get this template, if I attack this template, everything is gone.

So, it is a one way function because inverse you cannot we are assuming you cannot do it, even though now work is going on but inverse is difficult. So, if it is difficult, then you automatically you cannot regenerate the R O I. Because it is not invertible but but what we observe is that no. There is a possibility or you cannot prove that it is impossible, it is not possible. There is a possibility to regenerate. Once, I can regenerate my image or R O I, then I can do lot many things.

You think about this way, that I know that given minutiae points of a fingerprint; this is given or is known to you. If I manage to get R O I , then what happens? Once R O I is known, I can put R O I and get the fingerprint cap on rubber fingerprint cap. So that you can put it. Have you seen any episode in CID? Have you? CID? No, that is a morning time for you. CID? Nobody has seen CID? No?

All sustable thing you will find there. So, you know, what he has done in one episode, that from the template he has obtained the image R O I and from R O I he has gone to a person, who develops the molded materials. So, he got the fingerprints cap and he put the cap and he has done all the work. So, this is possible but only thing is that you have to understand the amount of effort is required for that. So, that is important, the amount of effort I have to put, that much my value must be much more than that whatever I am I am putting my effort. So, that is important thing.

(Refer Slide Time: 37:04)



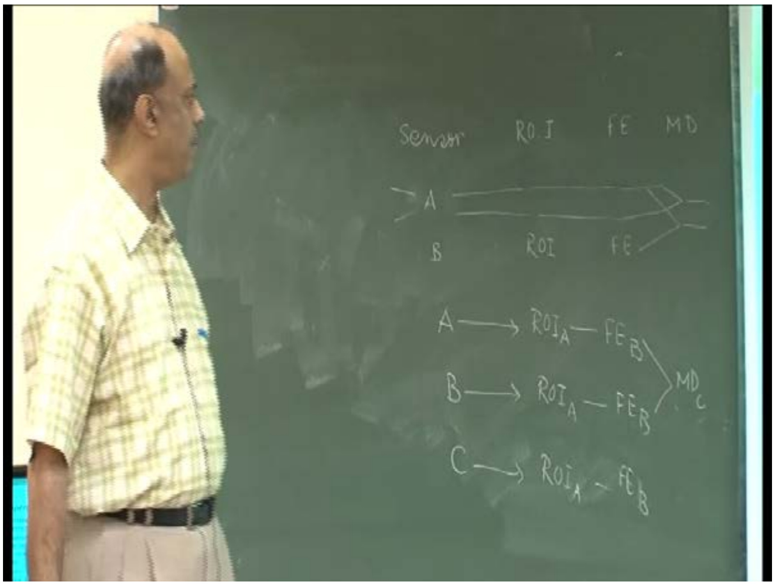
Interoperability

- Government applications of biometrics need to be concerned with interoperability.
- Biometric samples enrolled on one system must be usable on other vendor systems if a government is to allow cross-jurisdictional use, and to avoid vendor lock-in.
- However, recent work on interoperability has revealed it to be difficult, even when all vendors conform to standards.
- Such interoperability difficulties present biometric system vulnerabilities, which could be used to increase FRR or for a Denial of Services attack.

This is a big problem. This is we are all fighting like anything, everybody is fine. That nobody wants to be to get a system, which has the monopoly business. Say for example, then the vegetable supplier at your hostel, same vendor comes. What will happen? After time t, he will start cheating you. So, you have a committee. You decide that I will not accept the data or vegetables from him only. I want to get from some other people also.

So, that I am not depended on him. So, he cannot cheat me. Only issue is coming, that everybody has certain steps of or methods to follow to produce the output. Now, the method will be following for producing the output given the inputs same from the same area, he should be given the output properly but if I take the input from some other place, it should also give me the output. That is the thing, which is may not be possible.

(Refer Slide Time: 38:32)



For example, I have in my case that I have sensor, then I have R O I detection, am I right. Then I have to pre process extract enhanced the image, then you have the feature extraction, then you have the matching and finally, decision; matching and decision. This is the thing you have. Now, I have a sensor A and a person subject has come. On the same sensor, he has given the data. He will be getting the two R O I and two features will be extracted; finally, matching will be there.

Now, I have if I am dependent on him, then whatever lifelong I have to take his help. Because without him, I cannot survive. Say, suppose I introduce the biometric fingerprint biometrics in the bank and I decide that cost match is the supplier, then cost match, I will be dependent on Cost Match Company. Otherwise I will tell my sister will not run. So, the bank will tell nothing doing, I it should be free to be who from whom I will decide, I will get the sensor, my sister should work.

Now, what happens that I can introduce that, do that two system A and B. Now, from A, I will be extracting the R O I and from B also I will be extracting R O I. Then, it is F E. Finally, whatever features are there that should be matched and give the genuine output and if I use this two images using obtained from one scanner, whatever output you are expecting; if I use the true sensors to get the output image, I should get the similar match matching score. But in reality you will not.

So, what happens, that I have the two sensors. I have given one data here, same figure I have given here but while I have used. Now, R O I is his R O I and this R O I is extracted from this algorithm, features will be extracted from using this algorithm, features will be extracted within this algorithm. Now, these two features, even though you tell it is a, say particular standard is there, then also there is something hidden.

Somebody maybe using one byte information, somebody using four byte information, somebody maybe that from the centre onwards you are doing centre, then nearest neighbor and so on, somebody may be from the top one, all sorts of thing is there and matching algorithm, whose matching algorithm you will be using, whether his matching algorithm or this matching algorithm. To take the decision, that will also be coming in between but whatever it maybe the my matching score should be same or similar, to the other one. So, the problem becomes here.

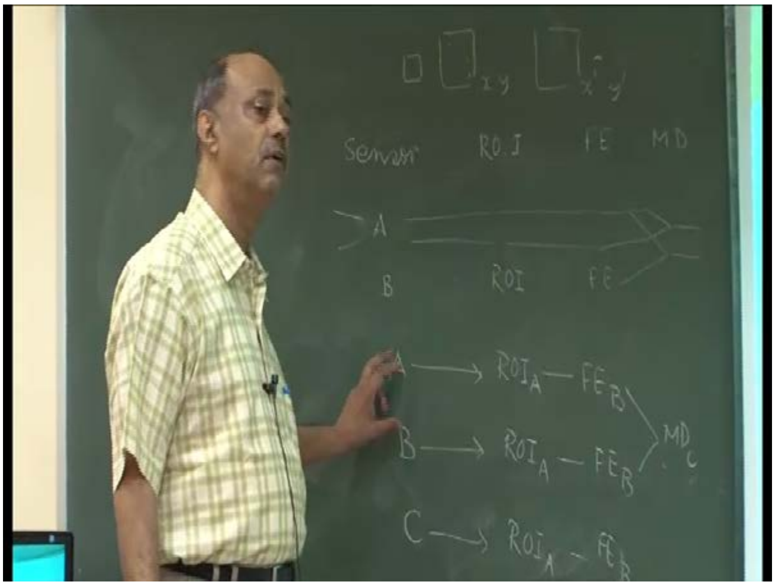
I have two, let us say three sensors. So, what government of India or any government expects? That one image I will be extracting from there, another image I will be extracting from here and I will be using; suppose, his R O I R O I of A to extract the image. I have extracted the image R O I from the R O I extraction algorithm of first one, then I must be able to use on this R O I feature algorithm of B. So, features are extracted using the algorithm B.

But I will be using the matching algorithm of C. If I do it and if I get the similar matching score, then I will be able to tell yes, all these three systems are interoperated. But this is not the case because you know every vendor has certain hidden things and certain proprietary things, which he does not want to which he does not want to share. Because in the standard in I S O, what we tell? We tell that you have to your algorithm should be on minutiae points. It should be on 500 d p i.

I cannot tell everything that you had to be do, the he had to follow this, this, this, then nobody would be able to do a business. Somebody has to prove that my algorithm is better than him. So, he has to do some work. So, that is hidden. So, in some scanner, image size is x coma y; another image size is not x coma y; it is x dash coma y dash. I am telling only 500 d p I or 500 p p I, 500 pixels per inch.

But I cannot extract, I cannot tell what is the what is the image coverage that is not defined.

(Refer Slide Time: 44:36)



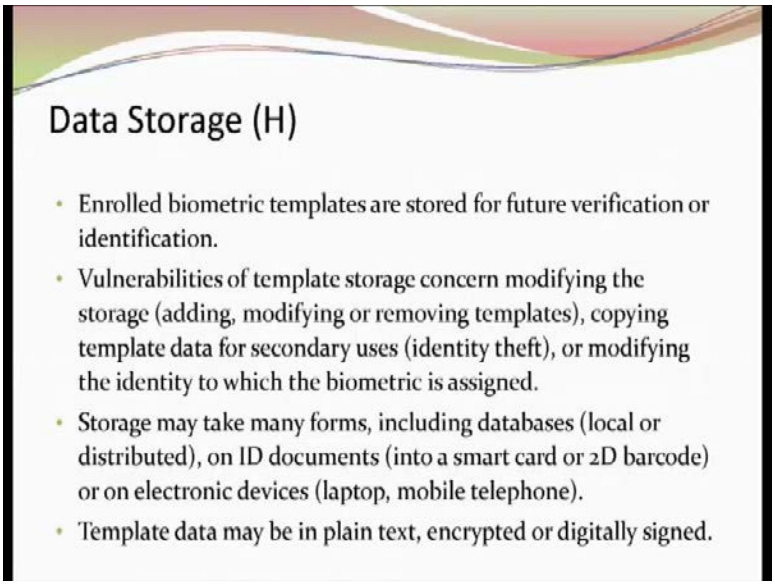
So, I have somebody is having the size x, y; somebody will have x dash, y dash and so on. Now, once I use this R O I, extraction algorithm, it may be dependent on F E, but I have to make it monopoly. He wants to make everybody wants to make his business monopoly because I am a businessman, I do not want others to enter into my area.

So, what I will do? I will read my data based on this fix x y. If it is a variable size, he is in problem. So, the system will not be able to detect properly R O I. This is first time. Suppose, there exist a system, which obtain reads the data of variable size. So, suppose the R O I can read the data at variable size. Now, which extraction will be coming?

Now, the features he is extracting from the variable size, we introduce too many false feature points. Because the smaller size; suppose, I have this one and another one image is very smaller size and this one he is habituated with the extract; the feature on the small value, where I have the larger area that he has extracted but he will get some small points here.

Because he his data is original data is this one. Now, you have asked to obtain the features from this size. So, false data will be coming. As a result, false match will come. So, enterable should be one, where the sensor of different type feature extraction algorithm I must get from somebody, some body may develop the R O I extraction algorithm, somebody should be able to design the matching algorithm. I must get the similar results. What I used to get from using only one sensor but this is not possible. As a result, you will find the error rate is very high. So, as a result, you will find the false rejection rate or false acceptance rate is very high.

(Refer Slide Time: 47:02)



Data Storage (H)

- Enrolled biometric templates are stored for future verification or identification.
- Vulnerabilities of template storage concern modifying the storage (adding, modifying or removing templates), copying template data for secondary uses (identity theft), or modifying the identity to which the biometric is assigned.
- Storage may take many forms, including databases (local or distributed), on ID documents (into a smart card or 2D barcode) or on electronic devices (laptop, mobile telephone).
- Template data may be in plain text, encrypted or digitally signed.

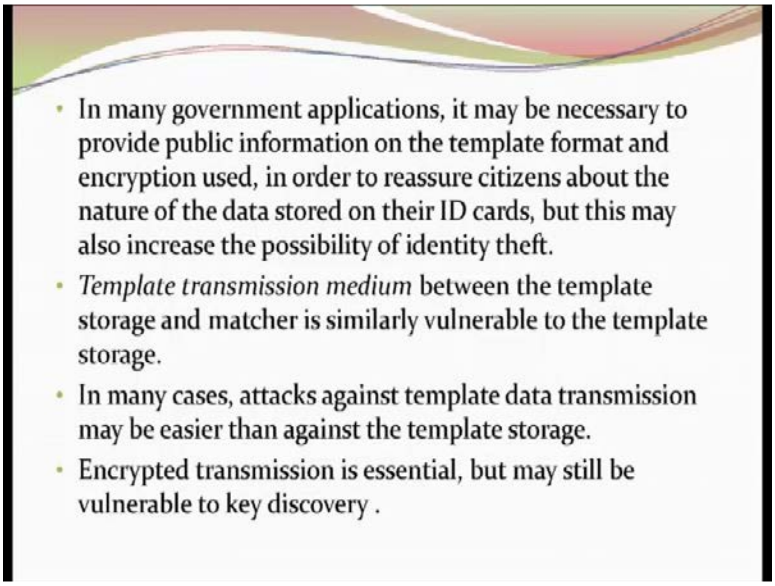
Now, the next one is the, you have extracted the features at the enrollment stage, you have to store the data into the database. How to store the data? because this will be used for verification and identification.

Now, in the data storage, also there are several ways you can think. One is that I can while storing the data; I will not take much time. I will give you 4, 5, 6 minutes. The data storage time, what I can do? I can what features you have extracted. I can add some other additional information in that, add some additional feature points. Or I can remove some, delete some of that. This is possible, very very simple. I just while storing, I put some extra things or I remove some of that. This is one level

Or I put the template into another area for secondary use and once, I put that into secondary storage into the feature into secondary area, then you are gone because your data can be taken by somebody else or I can modify your identity, even though you have given the your data, I have extracted the feature but while storing I am not storing your features. I am storing my features. I have extracted everything I have extracted. But once

I know that your ID is 35 and instead of storing your data, I will store my data. So, whenever you come to withdraw money, I will be also give my finger print and I will withdraw my money. Your money not my money. Then that is possible. So, there are people they think that this template can be encrypted.

(Refer Slide Time: 48:53)



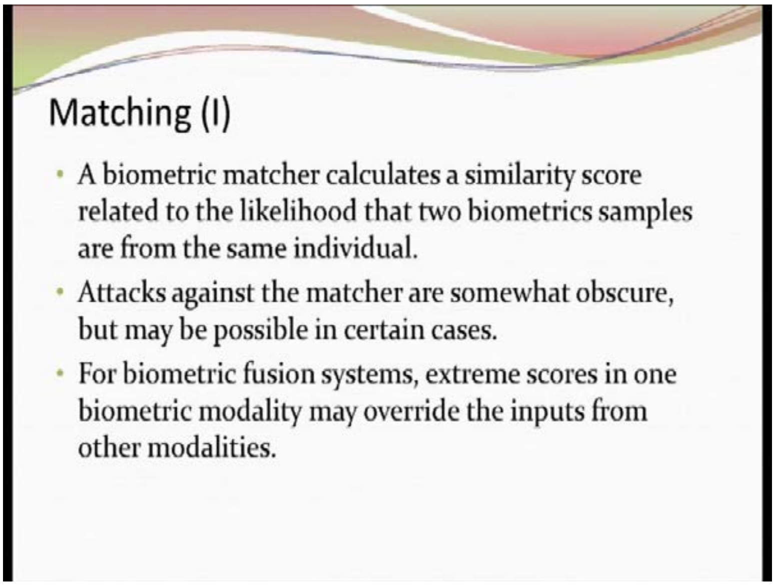
- In many government applications, it may be necessary to provide public information on the template format and encryption used, in order to reassure citizens about the nature of the data stored on their ID cards, but this may also increase the possibility of identity theft.
- *Template transmission medium* between the template storage and matcher is similarly vulnerable to the template storage.
- In many cases, attacks against template data transmission may be easier than against the template storage.
- Encrypted transmission is essential, but may still be vulnerable to key discovery .

Before storing, you just put encrypted. So that, this is not possible. Now, this is what happens? That even though, you store your data. Data means feature points but rule says that what information should be in public domain. Your name, your date of birth, your fingerprints all those things should be in the public, that is a government government (()). Then otherwise, what is the guarantee that you have not stole or you have not misused all my data. At the same time, I must know also that yes, you have put my data into the database. Because if I give my fingerprints, my name, I can generate.

And suppose my left hand fingerprint and I can match with his left hand, by replace that. So, all those things. So, I must know that, what are the features you I have put into this, should be available to the public and once, it is available so there is a chance of identity theft. So, in many cases, attacks against template data transmission may be easier than template storage. So, generally we do not. One way is that.

Instead of storing the modified data into the database while you come, I know that he has come. So, I will put. Suppose, I know that he has come to withdraw money and he has given his fingerprint to withdraw his money. So, that while he has given the data, I will see that that it has gone to somebody else. So, that is the template storing instead of storing on touching the template storage, you work at the time of transmission. I think two more parameters matching and decision.

(Refer Slide Time: 50:52)

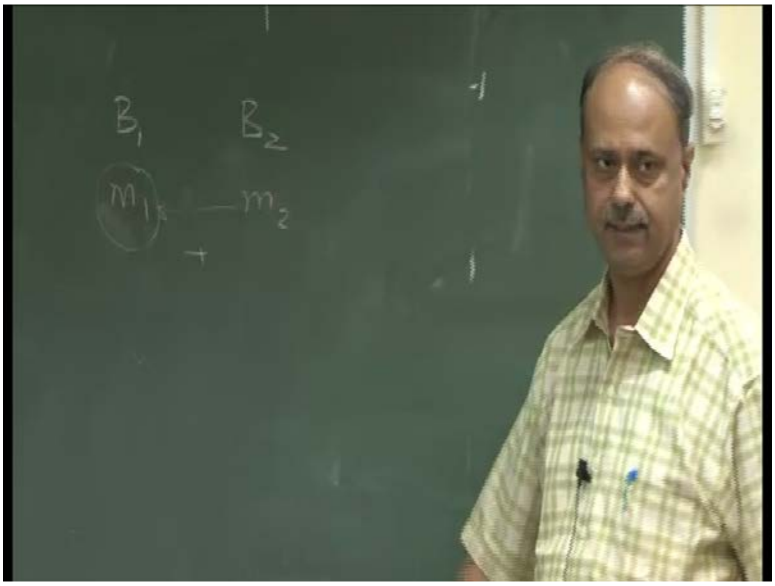


Matching (I)

- A biometric matcher calculates a similarity score related to the likelihood that two biometrics samples are from the same individual.
- Attacks against the matcher are somewhat obscure, but may be possible in certain cases.
- For biometric fusion systems, extreme scores in one biometric modality may override the inputs from other modalities.

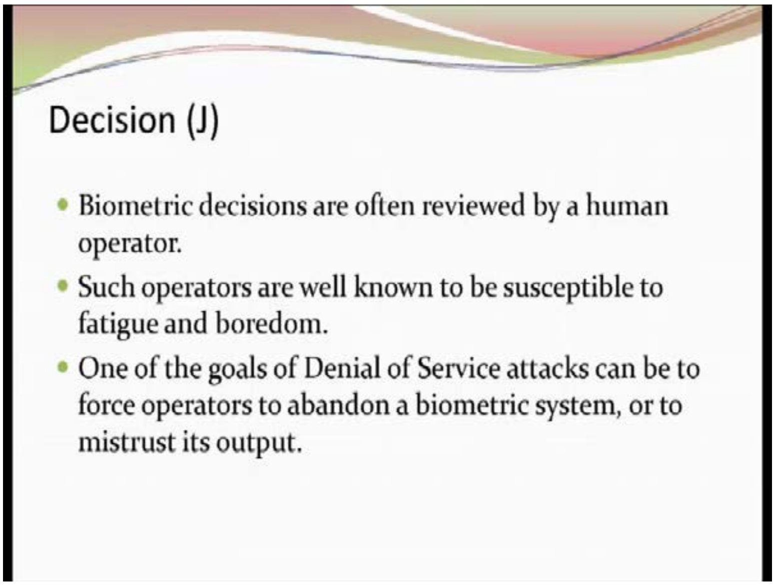
So, what biometric matching does? Given the two tablets, he matches and it tells that you okay. This is the matching score; no attack can be done there itself. What is the attack there? I can see that, even though the matching score is high forcibly by introducing some method, I can make it low. So, that is possible or what I can do? You have the. Suppose, I have the I want to fuse the multiple biometrics data, so you got a matching score here; you got matching score for this and this matching score is also replaced by this one. That is also possible. So, you may get different type of things.

(Refer Slide Time: 51:44)



Say, I have one system B 1, another system is B 2 and you got the matching score m 1,m 2. So, if I fusion is just addition of too many matching score, I should mean that both of them are normalized similarity or dissimilarity things. So, I add it, I get one matching score. This is one way I get. But what I can do? I can attack by replacing this one by this number itself. Simple way; nothing; I have not done anything. This can be done very easily and you will be able to reject or accept or you can get very good matching score.

(Refer Slide Time: 52:23)



Decision (J)

- Biometric decisions are often reviewed by a human operator.
- Such operators are well known to be susceptible to fatigue and boredom.
- One of the goals of Denial of Service attacks can be to force operators to abandon a biometric system, or to mistrust its output.

The other one is the decision. So, even if you get the matching score, now you have to take that decision, whether it is accepted or rejected. And if I because it is the last component, after that a person will be allowed to enter or will be rejected. So, what do we do? I can stop you to enter by increasing the threshold value. Simple, nothing else. So, I put in my database, if this, this, this, this ID is there, then their session value is very high in my system.

So, if you come 35, I given your that everything is true; at the time of matching score, you got a very high matching score but I have put one condition that for 35 session value is this. So, you are out. Or I can do some manipulation because operator is involved in between. That operator will be coming. So, you will be coming, you will be giving the data and you want to get money and operator will put some indication, that yes I do not want his case should be considered. So, he put some key there or which indicates that he was the high session value for a similarity match and you will be out. So, after time t, after several transactions you will be told that no no you cannot get money. That is possible.

Or you can always tell no no, this is not giving me good result. So, I should reject this system. You get another system, which is compromisable, you can compromise with that and you can get the better deal out of it. So, these are the different types of attacks possible on different modules and interconnection between the two different steps.