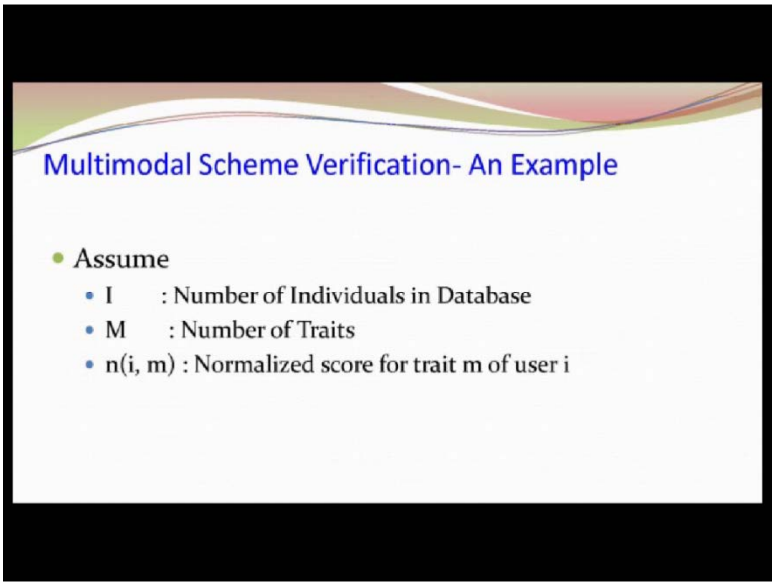
Biometrics

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

Lecture No. # 15

(Refer Slide Time: 00:17)



Multimodal Scheme Verification- An Example

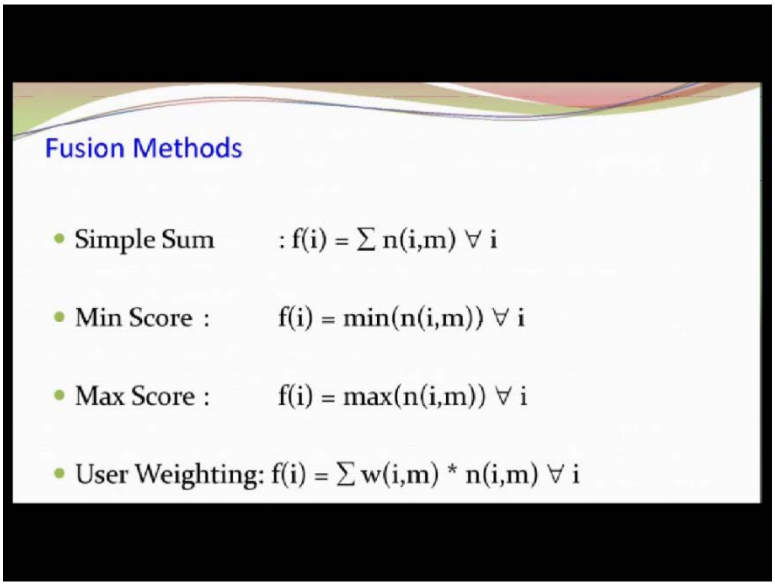
- Assume
  - I : Number of Individuals in Database
  - M : Number of Traits
  - n(i, m) : Normalized score for trait m of user i

Today, we want to discuss about how a given multimodal environment here we are looking for that suppose I have the two biometric traits or more biometric traits and how to compute the false acceptance rate and false rejection rates? Because I know the false acceptance rate of one system based on one type of database, and another biometrics trait I have, its false acceptance rate and false rejection rates are known based on one another data base.

Now, how to combine these things to get the false acceptance rate and false rejection rate for the combined one? Now, first let us understand that how to fuse my biometrics data. So, here this fusion I will be talking based on the score level fusion and what are the various techniques I can use to fuse these scores? So, I is the number of individuals, number of subjects in your database, M is the number of traits.

Suppose, there are M traits you have selected for fusion and n (i,m) that for this trait of the user I that is the normalized score. Now, why I am telling normalized score? As I told you the scores will not be lying between 0 and 1, some score will be lying between 0 and 1000, some will be plus x to plus y, some will be minus x to plus y, some will be in decimal format, some would be in the integer format all those things some will be (( )) score and so on. So, all of them should be brought under one umbrella so that you can combine them. So, that is why we have normalized it. Then n (i,m) that means the normalized score for the trait M of the user I.

(Refer Slide Time: 02:23)

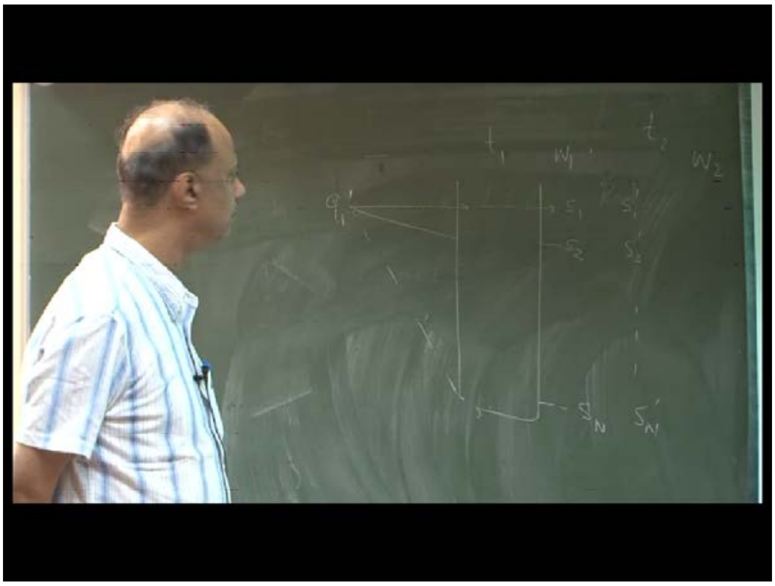


Fusion Methods

- Simple Sum : $f(i) = \sum n(i,m) \; \forall \; i$
- Min Score : $f(i) = \min(n(i,m)) \; \forall \; i$
- Max Score : $f(i) = \max(n(i,m)) \; \forall \; i$
- User Weighting: $f(i) = \sum w(i,m) * n(i,m) \; \forall \; i$

So now the scores are normalized. So for one trait I got.

(Refer Slide Time: 02:34)



What happens here? I have a database of trait I, say trait 1 and a query q 1 has come. So, q 1 will be compared with this and I got some score S 1, q 1 will be compared with this I got score S 2 and here I get score S N. For this query 1 I got those various scores. Now, this has been normalized.

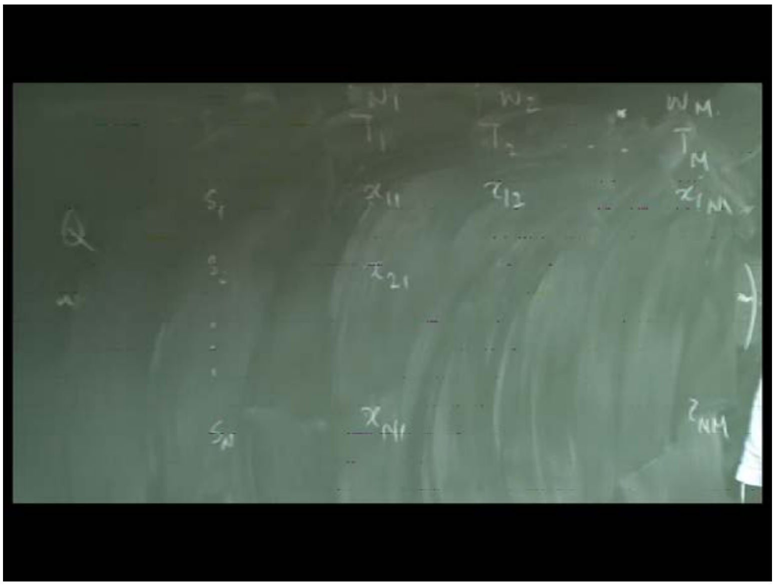
Similarly trait 2 you will be getting similar type of score say S 1 prime, S 2 prime and S N prime such types of things that M(s) are traits are there. Now, these are normalized first simple way is that I add the scores. Because, these are all the scores some unitless number I add them, and then I tell this is the score of this subject compared to this. This matching between these two trait has the scored this.

Another one is that no I decide the minimum of this score I want because I am very conservative. I want to take the minimum of this score. Another could be that no I am generous I will take the maximum of this. And, another one is the weighted average I can take that I give for each score I give some weights. For trait 1, this weight is W 1 for trait 2 weight is W 2 and so on. So, W 1 into the score plus W 2 into the score and so on that will give you the total score.

So this basically the weighted average I want to take. Is this clear?

Sir in S 1, S 2, S N first we select the best S 1 from S M.

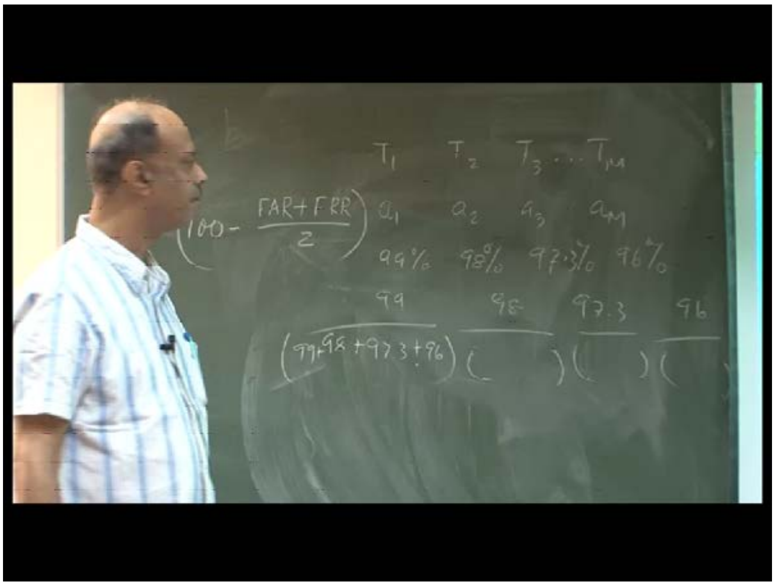
(Refer Slide Time: 04:43)



First m see, I have a query Q. I have the subjects S 1, S 2, S N. I have trait T 1, T 2, T M so, Q is compared with S 1 I get a score. Q is compared with S 2 I get another score, compared to S N I get a score. Q is compared with S 1 against the trait 2, I get a score. Similarly, I get x N here, I get x N M. Now, all these scores are normalized 0 to 1. Now, if I sum them then I get one score, that score is the score between these two. If I sum them I get a score this is score between Q and S 2 and so on. Or I can think that no minimum of this will be giving you the score or maximum of this will give you that this.

Another one is that no I want the weighted average. I put some weight against here some weight W 1 here W 2 and here W M. So, this into this plus this into this plus this into this well some of the weight is one. Now, the question you will be thinking that how to get the weights?

(Refer Slide Time: 06:21)



So the weight can be given as say I have the T 1 T 2 T 3 T M. These are the things and I have the accuracy a 1 a 2 a 3 a m this accuracy is known to you based on our trading data set. Test data set where you have obtained the F A R and F R R. These are known against each trait for a trading data set yes this is known.

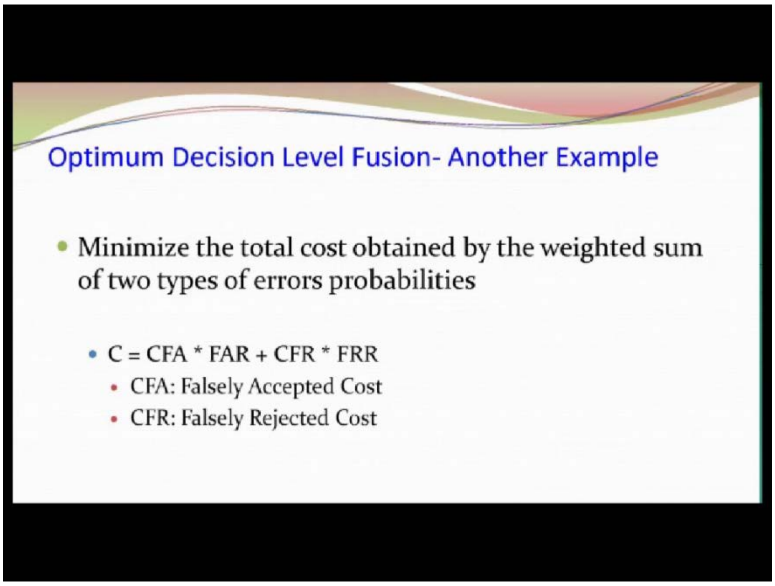
So as I told the accuracy is nothing but this will give you the accuracy. So, for each trait you get the accuracy. Now, let us assume that this is 99 percent, this is 98 percent, this may be 97.3 percent, this may be 96 percent and so on.

Now, I have to assign the weights so since this is giving the highest accuracy I should give little weight compared to this. So, I can put 99 divided by 99 plus 98 plus 97.3 plus 96. Similarly, you put 98 divided by these weights 97. 3 this 96 point this. So, you get the corresponding weights and that weights you can assign the W 1 W 2 W 3 W M is it okay?

But, this is an example I am giving you. There may be other ways to assign that but what we are doing we are putting the weights like this. Now, another issue may come up, because in reality it happens. See, what we have assumed that everybody has given the data of M traits but in reality it is not true. Some of I have given first 10 traits data, some of them here here like that because somebody may not be able to give the data on the spot his I D is not available some of them the day I went to collect the data he was not available and like that it may occur.

So, some of them will be 0 here. But that does not mean that it is not matched. It indicates that man is absent you can some put some other value minus infinity or something like that and correspondingly that weight has to be adjusted correspondingly that weight has to be adjusted. Am I right? Is it clear? You should not think that suppose it is minus infinity and you are assigning W then you are making mistake W 1 W 2 into minus infinity give you the minus value. So, if this is minus and if you do not consider and the weights these weight will be adjusted among them. So that the sum of weights is 1 is it clear? Yes.

(Refer Slide Time: 09:55)

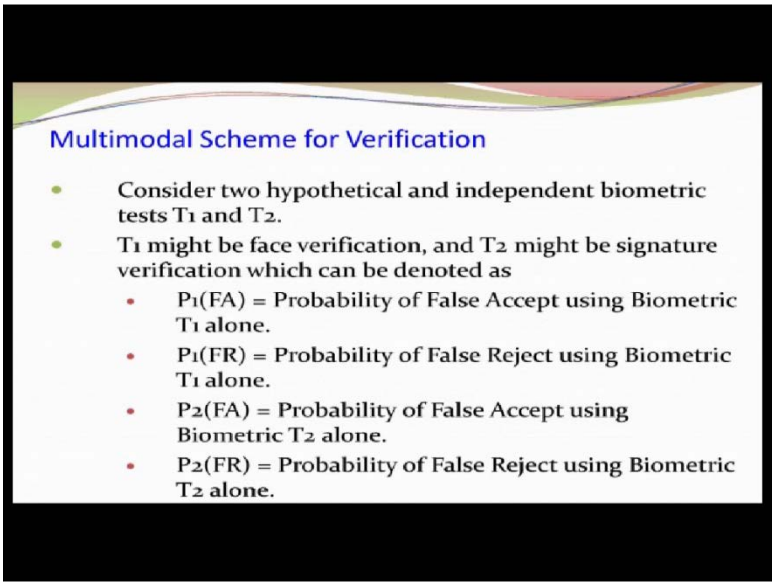


Optimum Decision Level Fusion- Another Example

- Minimize the total cost obtained by the weighted sum of two types of errors probabilities
  - C = CFA * FAR + CFR * FRR
    - CFA: Falsely Accepted Cost
    - CFR: Falsely Rejected Cost

Now, suppose I want to introduce the cost on it. Then cost for the false acceptance into false acceptance rate plus cost for false rejection into false rejection rate and then you can obtain what is the cost what is the cost of your system? So, sometimes you may have to look for the minimum cost suppose I introduce here again cost is also involved in that. Then, cost becomes your weight. So, cost into this cost will be your weight. So, that cost you have to take into account in your computation.

(Refer Slide Time: 10:18)



Multimodal Scheme for Verification

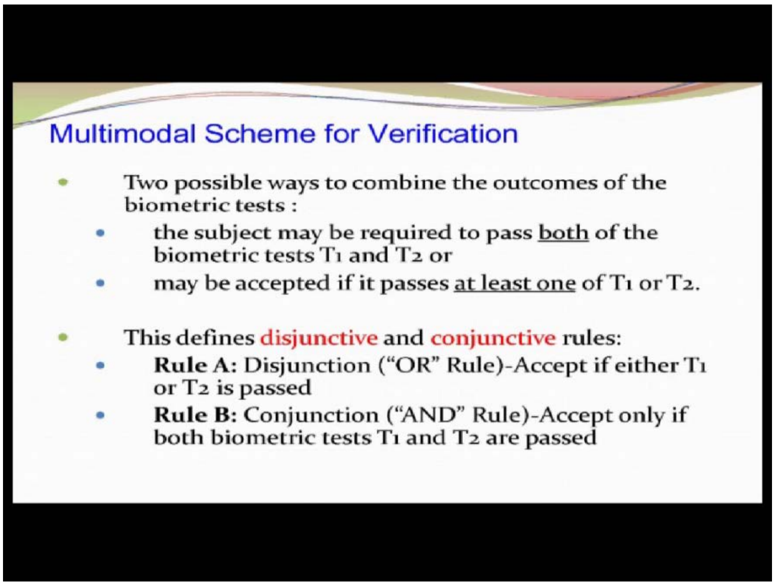
- Consider two hypothetical and independent biometric tests T1 and T2.
- T1 might be face verification, and T2 might be signature verification which can be denoted as
  - P1(FA) = Probability of False Accept using Biometric T1 alone.
  - P1(FR) = Probability of False Reject using Biometric T1 alone.
  - P2(FA) = Probability of False Accept using Biometric T2 alone.
  - P2(FR) = Probability of False Reject using Biometric T2 alone.

So, by now you know that how to fuse the score? Also you know what is the false acceptance rate and false rejection rate. Now while you will be telling that I have the M number of biometrics traits for each of them this is the false acceptance rate and false rejection rate. You have to tell now what is your expected false acceptance rate and false rejection rate for the fused one. Fuse result you have to tell that.

So, here for simplicity let us consider there are 2 biometrics traits they are independent. Independent means that one is say face another may be finger prints. They are independent, they are not related it is not that one is left eye another one is also left eye, but by another camera or another sensor. It is a two different one, one is the face another one is finger print or something like that.

And we want to compute we want to compute the false acceptance rate and false rejection rate for the fuse results. Now, P 1 F 1 let us assume that this is the false acceptance rate for the first trait, first trait may be trait T 1 and P 1 F R is the false rejection rate for the trait T 1. P 2 F A is a false acceptance rate for the trait T 2 and P 2 F R is the false rejection rate of the trait T 2.

(Refer Slide Time: 11:59)



Multimodal Scheme for Verification

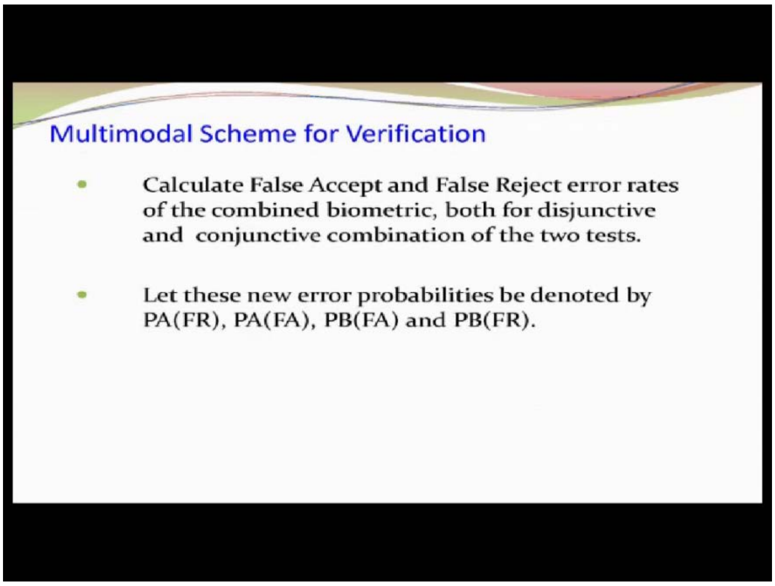
- Two possible ways to combine the outcomes of the biometric tests :
  - the subject may be required to pass both of the biometric tests T_1 and T_2 or
  - may be accepted if it passes at least one of T_1 or T_2.
- This defines disjunctive and conjunctive rules:
  - **Rule A:** Disjunction ("OR" Rule)-Accept if either T_1 or T_2 is passed
  - **Rule B:** Conjunction ("AND" Rule)-Accept only if both biometric tests T_1 and T_2 are passed

Now, there are 2 possible ways you can combine the scores or you can combine the results. The 2 possible ways to combine the outcomes of the biometric test say one possible way is that in both the case the person has to be successful, has to be accepted. This is the decision level fusion I am talking that in both the test therefore test T 1 for the trait T 1 he should be accepted and for trait T 2 also he should be accepted, then he is through.

Another method will be that no if he is pass in one of them then he is accepted. Pass in of them means if he is accepted by one trait irrespective of the result of the other one he is through. These are the two possible ways you can fuse at decision level.

So, there are two rules one rule is that conjunctive rule or AND rule. Here it is telling that the subject has to be passed or accepted by both the tests and dejective is the OR rule where the subject will be accepted if and only if he has passed in at least one of them. These are the two things remember, what we have considered the both the traits are independent.

(Refer Slide Time: 13:26)

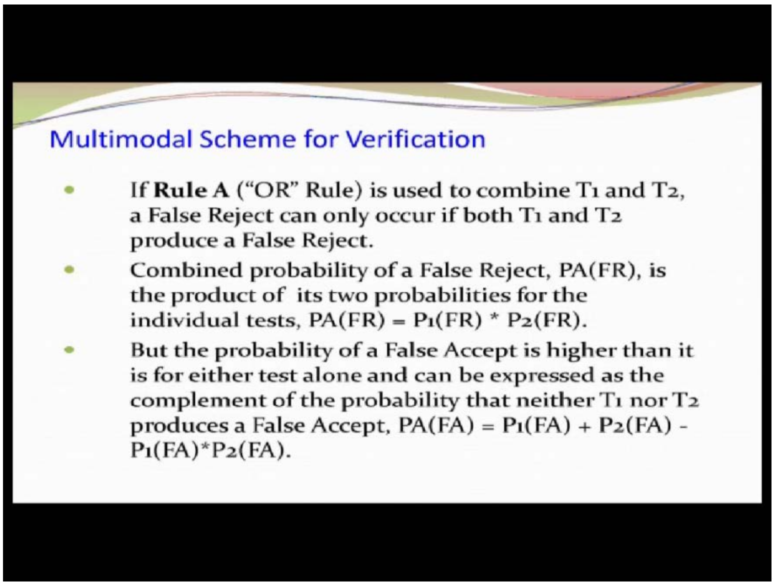


Multimodal Scheme for Verification

- Calculate False Accept and False Reject error rates of the combined biometric, both for disjunctive and conjunctive combination of the two tests.
- Let these new error probabilities be denoted by PA(FR), PA(FA), PB(FA) and PB(FR).

Now, we want to calculate the false acceptance rate and false rejection rate of this combined biometrics. Let us assume that P A is the false rejection of the first case A and B. False acceptance rate false acceptance rate of the conjunctive conjunctive case and false rejection rate of the conjunctive rate and here it is the dejective one and this is the false rejection rate of the dejective one.

(Refer Slide Time: 13:59)

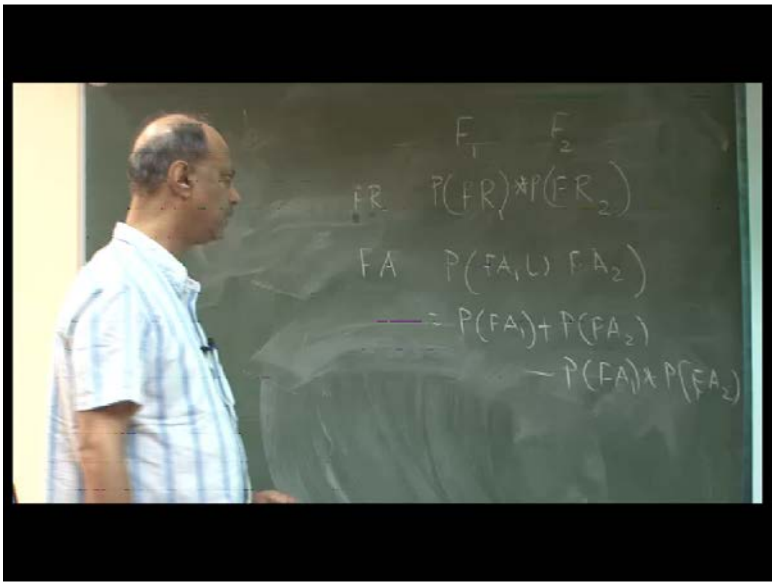


Multimodal Scheme for Verification

- If **Rule A** ("OR" Rule) is used to combine T1 and T2, a False Reject can only occur if both T1 and T2 produce a False Reject.
- Combined probability of a False Reject, PA(FR), is the product of its two probabilities for the individual tests, PA(FR) = P1(FR) * P2(FR).
- But the probability of a False Accept is higher than it is for either test alone and can be expressed as the complement of the probability that neither T1 nor T2 produces a False Accept, PA(FA) = P1(FA) + P2(FA) - P1(FA)*P2(FA).

Now the rule A is telling that it is the OR Rule.

(Refer Slide Time: 14:10)

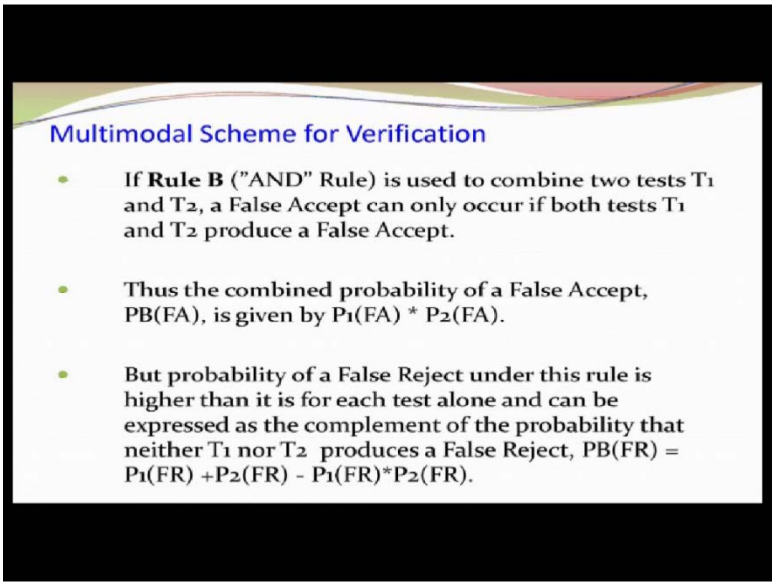


A person will be rejected only when both the case it is failed. See, OR rule means what? If he is accepted by one of them you tell that he is accepted, he is the genuine person. So, OR rules tells that in both the cases he has to be fake. So, in order to obtain the false rejection rate this case, so he has to be falsely rejected here and he has to be falsely rejected here. If, they are rejected then the false rejection will be and but both of them are independently distributed.

So, probability of false rejection rate and probability of false rejection rate this will be multiplied and that will be your false rejection rate because they are independently distributed. So, I just multiply these two I get false rejection rate of the combined one. So false rejection rate is nothing but the product of the false rejection rate of the two traits because both of them are independently distributed.

Now, what happens in the case of false acceptance for this case? See that means, he will be falsely accepted by one trait, he will be falsely accepted by another trait and there is a common thing also that he has been falsely accepted in one trait and also in another trait. So, it will be nothing but probability of false acceptance A 1 union which is nothing but weight of false acceptance rate 1 plus minus; so this plus this minus this because they are independently distributed. So, this is formula for the computation of false acceptance rate.

(Refer Slide Time: 16:33)

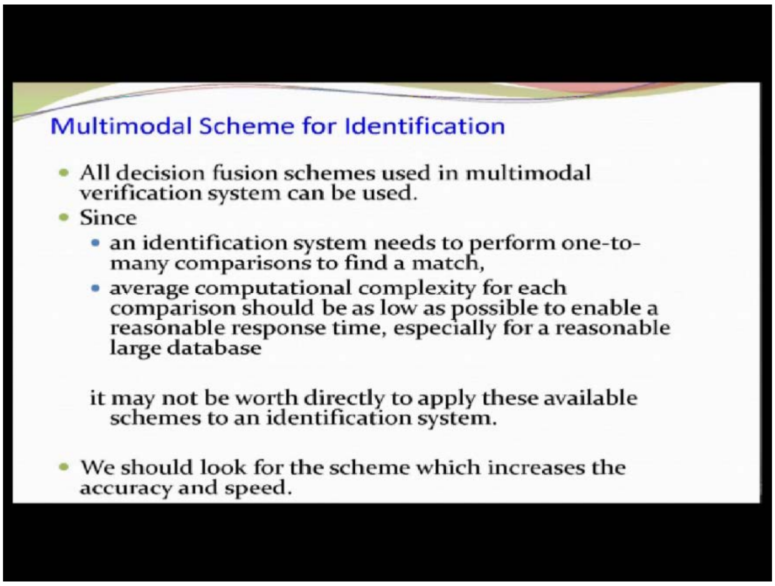


Multimodal Scheme for Verification

- If **Rule B** (”AND” Rule) is used to combine two tests T1 and T2, a False Accept can only occur if both tests T1 and T2 produce a False Accept.
- Thus the combined probability of a False Accept, PB(FA), is given by P1(FA) * P2(FA).
- But probability of a False Reject under this rule is higher than it is for each test alone and can be expressed as the complement of the probability that neither T1 nor T2 produces a False Reject, PB(FR) = P1(FR) +P2(FR) - P1(FR)*P2(FR).

Now if the rule is AND rule, AND rule means that he will be falsely accepted only when both of them in both the traits he is falsely accepted. A person will be falsely accepted only when, he has been accepted falsely in both the traits. And both of them independently distributed so, the formula is P 1(F A) plus star P 2 (F A). And similarly, you can obtain the formula of other case the falsely rejection. Just you replace this one by that formula you will get it.

(Refer Slide Time: 17:21)



Multimodal Scheme for Identification

- All decision fusion schemes used in multimodal verification system can be used.
- Since
  - an identification system needs to perform one-to-many comparisons to find a match,
  - average computational complexity for each comparison should be as low as possible to enable a reasonable response time, especially for a reasonable large database

  it may not be worth directly to apply these available schemes to an identification system.
- We should look for the scheme which increases the accuracy and speed.

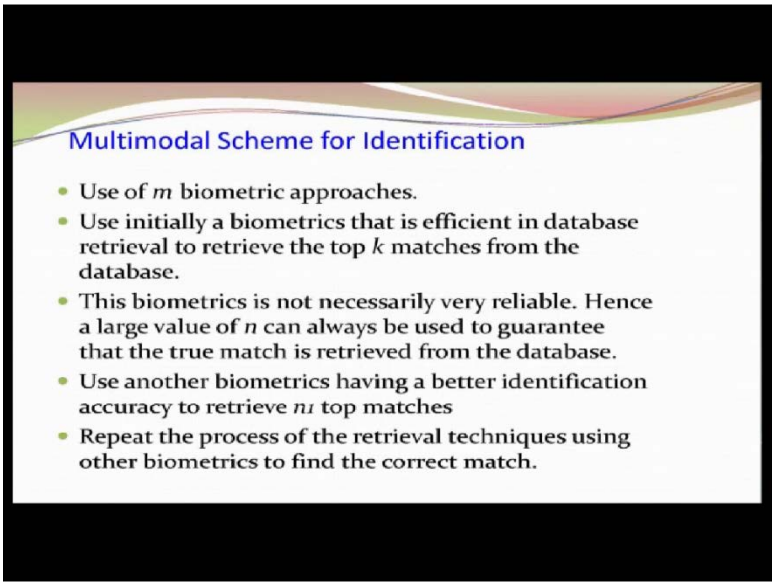
Now, think about whatever I discussed that is for the multimodal biometric system for verification. Now, let us think about the identifications. So, whatever method you follow for verification can I use it for identification? Say, what I have done for verification? I get a query and corresponding subject you have gone and by matching you got the matching score and based on some threshold value you tell yes or no.

So suppose, he is the person and you have compared with this you got the matching score matching score matching score and based on some threshold value you will be taking that accepted accepted rejected rejected accepted. Finally, you have drawn the conclusion.

Now, in the identification what I can do? I can also do the same thing that I repeat the same process one by one because identification means one(s) to end match. So I will be comparing this with this then, this with this then this with this and so on. And you follow the same method what you have done in the case of verification. So, verification is the particularly same process you are following only the individually on this I D you will be doing it here, you do not know the I D you will be testing against all of them.

So the same process can be repeated to draw the conclusion. But here you have the big problem. Because you have to compare everything so, time is the constraint. So, if you can if you can control your response time and moderately the number of comparisons then, you are through. So, that is the that is the reason why that exactly same method you may not be able to use it. You may have to think a little different way so that even though you follow the same operations but you have to reduce the search space so that moderate number of comparisons can be done.

(Refer Slide Time: 19:35)

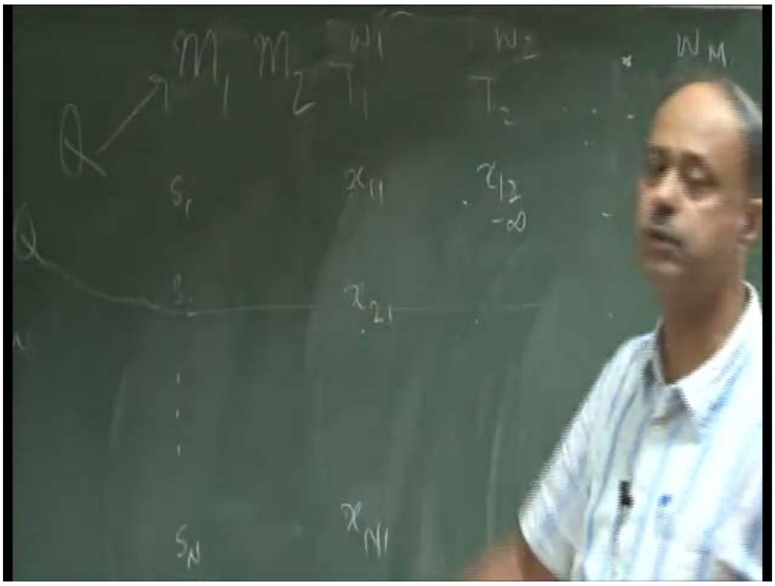


Multimodal Scheme for Identification

- Use of m biometric approaches.
- Use initially a biometrics that is efficient in database retrieval to retrieve the top k matches from the database.
- This biometrics is not necessarily very reliable. Hence a large value of n can always be used to guarantee that the true match is retrieved from the database.
- Use another biometrics having a better identification accuracy to retrieve n_1 top matches
- Repeat the process of the retrieval techniques using other biometrics to find the correct match.

So, what are the different ways you can think about it? The first one is known as sequential method. What it does? Suppose, you have M traits; of course, you know that which one is the costliest one and which one is the cheapest one you can arrange them. Or you can arrange with respect to the accuracy or you can use another method so as to arrange them with respect to the time requires based on that you decide. So what happens that you have got a query image and you arrange with respect to the cheapest to costliest one.

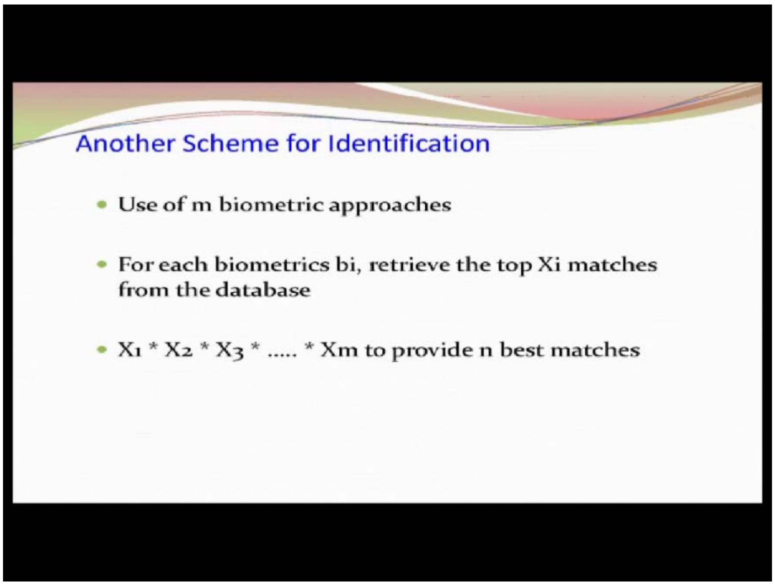
(Refer Slide Time: 20:39)



So, you use the query and use the cheapest biometrics trait and you select top m 1 elements subjects that they are likely to be matched. Now, you take the next costliest trait and you use that q query with this many subjects. Because they are no longer remaining n minus m 1, they are not belonging to my search area.

So, Q 1 will be compared with these m 1 elements and get the top m 2 subjects. Next level what you do? You take the next trait, next trait means next costliest trait and Q 1 will be compared with this m 2 subjects and get the top m 3 subjects and so on. So, if you continue after m traits you will be getting that some x number (( )) who are the probable candidates and who are passed against these many traits. This is a sequential method here, there are several issues you can think. First problem is that by if any means a person has been falsely rejected in the beginning, he is rejected he is out from the race. There is now way you can get him.

(Refer Slide Time: 22:25)

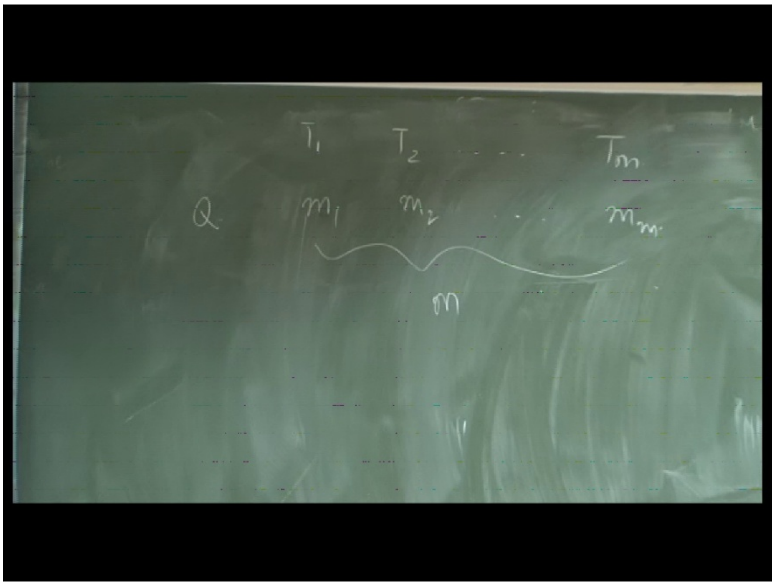


Another Scheme for Identification

- Use of m biometric approaches
- For each biometrics bi, retrieve the top Xi matches from the database
- X1 * X2 * X3 * ….. * Xm to provide n best matches

Another one is the parallel method.

(Refer Slide Time: 22:40)



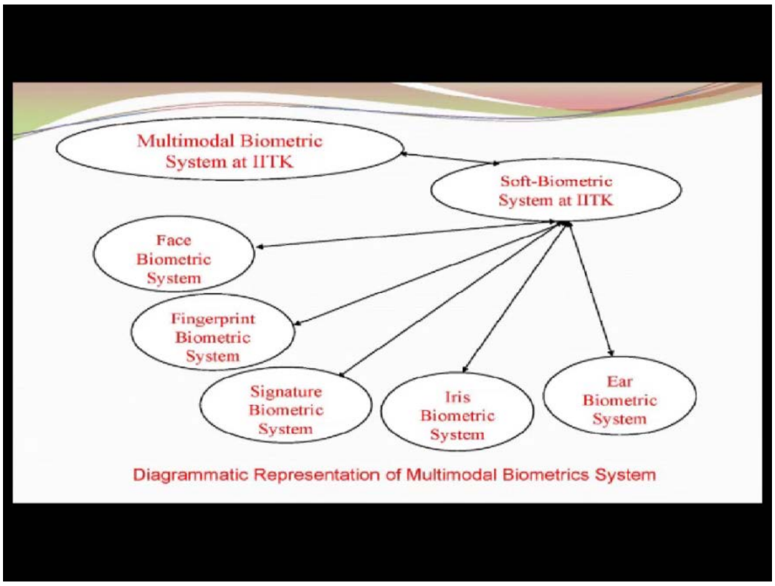
So what I do here? I have a trait T 1 T 2 T m and you have query Q and this query q will be matched against everybody. Pick up top m 1 elements or m 2 elements m m elements and then combine these to get best m of them. Best m of them means there will be some of them common. A person is lying in all of them.

He is one of the top most probable candidates. You will find one of them he is not been caught here but in the remaining he has been found he may be the second best and so on. So you get the m 1 of them m 2 of them m m of them and then obtain the intersection to get the top m elements. So, it has also some positive thing the person who has been missed out, he will not be missed out here. But, what you are losing that you have to do 1 to m comparison for each cases.

Now, another way one can think one can think is that why not the hybrids approach? Some of them some of them you go for the low cost one you go for total and for high cost one you do not go for the total. Because low cost one, it will be throwing those people, who are not at all a member of this. And, a slight match he will be in, you can take that a slight match means see a person will be out falsely rejected because of the threshold value only he will be falsely rejected. So, there will be some matching score will be there, it is not that it will be near 0, it will be near the threshold value.

So, if you follow this method those people will be in. And, through hybrid approach you put the costliest one to determine, who are actually member of that? That will be known, if you follow that method.

(Refer Slide Time: 25:13)

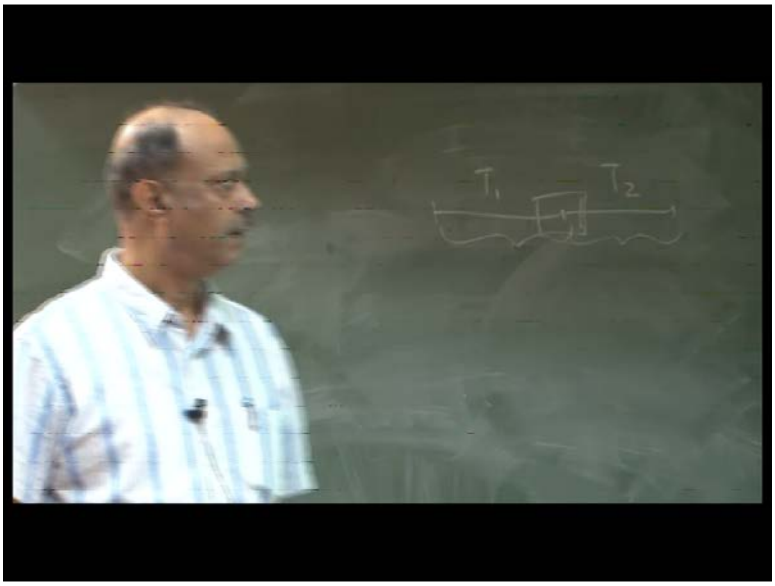

Multimodal Biometric System at IITK
Soft-Biometric System at IITK
Face Biometric System
Fingerprint Biometric System
Signature Biometric System
Iris Biometric System
Ear Biometric System

Diagrammatic Representation of Multimodal Biometrics System

Now let us talk little about our work here. What we have done? There is a concept of soft biometrics that will be discussed. Why we need the soft biometrics? Why we will be telling this when we discuss how to reduce the search space? Now, we have the face biometric system, finger print biometric system, signature iris, ear and so on and all of them gives you the score and (( )) them to get a fuse score and based on the threshold value you decide whether he is accepted or rejected.

Also sometimes what we do? That we obtain the features here, features here and then we combine all the features to get one features and use that feature for matching purpose. In some cases, the number of variables in the feature points or number of feature points against a feature vector may not be fixed, it may be variable. So, corresponding adjustment is required.

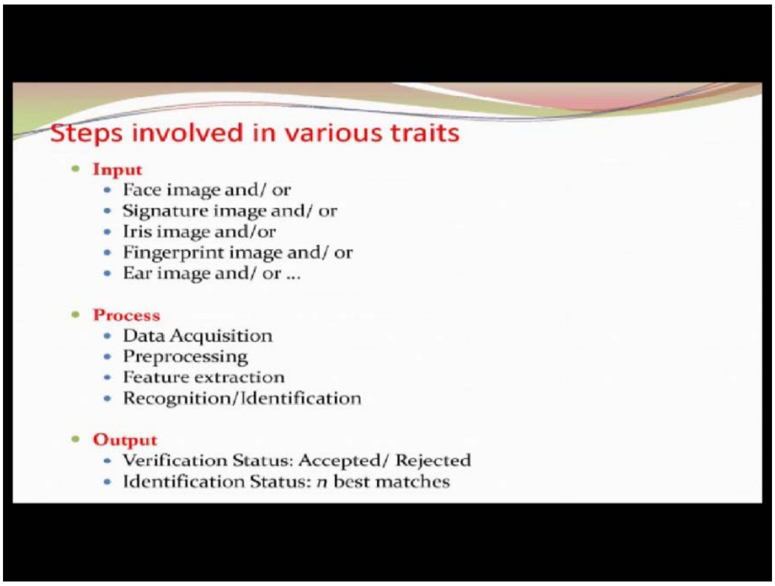
(Refer Slide Time: 26:25)



Otherwise, what happens? Suppose this is the feature vector for trait T 1 and this is the feature vector for trait 2 and here there may be a chaos condition. So what you have to do? You have to make it fixed. Otherwise otherwise, you will not be knowing whether this feature vector is for this or this one. So, some method you have to follow to keep track that this is the feature element for this feature trait and this is for that other one.

And, also you have to keep it in mind that this feature vector also should be such that they form similar type of (( )). See one is on binary pattern another one is on real domain, then there may be little problem to represent the data. So, you have to be careful that if it on real domain then if you put the binary pattern concatenation may not be a good way you can do it. Because this is 4 byte information and this is only 1 bit information so, it may be little problem. So, we have done on feature level and also on score level. Decision level we have not done much work and also not on sensor level fusion.

(Refer Slide Time: 27:32)



Steps involved in various traits

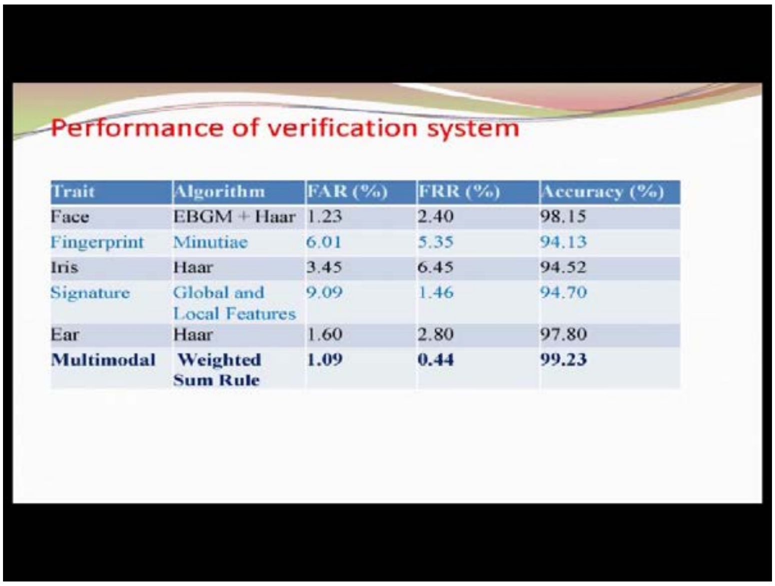
- **Input**
  - Face image and/ or
  - Signature image and/ or
  - Iris image and/or
  - Fingerprint image and/ or
  - Ear image and/ or ...
- **Process**
  - Data Acquisition
  - Preprocessing
  - Feature extraction
  - Recognition/Identification
- **Output**
  - Verification Status: Accepted/ Rejected
  - Identification Status: *n* best matches

Now, what you have in input? Input you have some images of different traits. It is not necessary that face image and signature image this way we will be getting. Some of them will be there; some of them will not be there. And, this is true for any pattern recognition problem that you have to get a data acquisition system; you need to have the preprocessing. Preprocessing means that you need to do certain type of correction say for example, I have to get the region of interest. Because I have taken a photograph where your face is there, neck is there, background is there. I do not need your background, I do not need your neck and other things only I need your face so, I have to extract this feature regions.

So if I give you the hander data I do not need the whole hand data, I need only the palm area so, the palm print or just region of extraction is required. Then lot many noises different types of noise may be there. So, those noise you like to eliminate but you have to keep it in mind that you are not you are not losing the features, because sometimes a feature can looks like a noise. You have to also ensure that there is a need of stretching the contrast so the features can be visible.

So those operations you will be doing in this case. From that image from that image you have to extract the features different types of features will be coming that, will be as that we will be doing the term paper you will be knowing all these things. And finally, matcher is required to match and draw the conclusion whether it is matched or not?

(Refer Slide Time: 29:27)



Performance of verification system

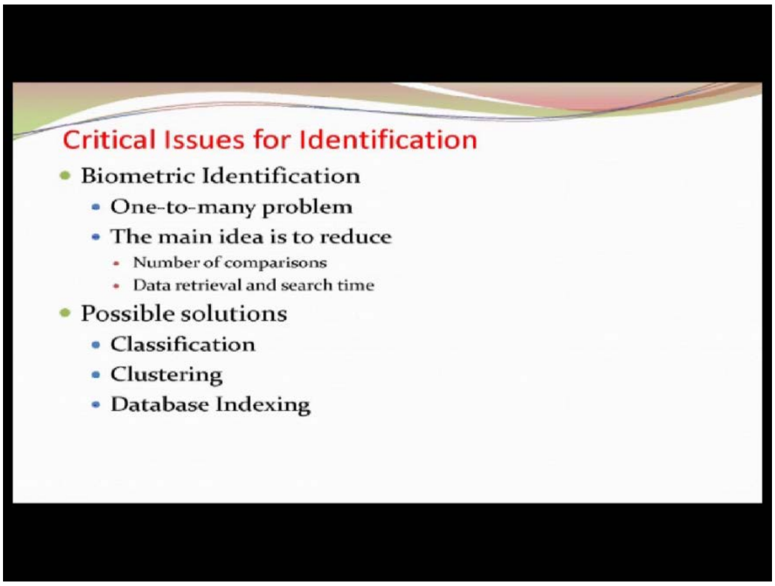
Trait	Algorithm	FAR (%)	FRR (%)	Accuracy (%)
Face	EBGM + Haar	1.23	2.40	98.15
Fingerprint	Minutiae	6.01	5.35	94.13
Iris	Haar	3.45	6.45	94.52
Signature	Global and Local Features	9.09	1.46	94.70
Ear	Haar	1.60	2.80	97.80
Multimodal	**Weighted Sum Rule**	**1.09**	**0.44**	**99.23**

So, so this is clear. So, some of you possibly will be working on this in the term papers, some of you will be doing working here or here. So this is accuracy level in our system. So, what we expect from you that your results, whoever will be doing the recognition things result should be better than this.

So, this is the bench mark for you so, I want better than this. And if you get the better results I can assure that 5 additional marks also I can give against your end term. So, everything is given 5 additional marks subject to the condition it cannot exceed 100 marks that is the thing. So, data set is given to you, everything is given and I do not want this one because this is not under your (( )) you take one of them any one of them some of you have taken iris already, some you have taken finger prints and other things.

Signature also we have not given you. Face I think some of you are working so, you take the challenge there is nothing because they are achievable 94 percent is achievable up to 96 it is achievable, only thing is you need little extra effort.

(Refer Slide Time: 30:52)



Critical Issues for Identification

- Biometric Identification
  - One-to-many problem
  - The main idea is to reduce
    - Number of comparisons
    - Data retrieval and search time
- Possible solutions
  - Classification
  - Clustering
  - Database Indexing

And, that is the reason why mentor wants to sit with you? Mentor wants to discuss because they are have also interest to achieve more than this. Now, in the case of identification, verification data is very simple. So after that boy left from my room I felt bad I should have shown him the answer books. So, the critical issues for identifications see these are one too many problems as this issue is number of comparisons how many comparison I have to give? How to retrieve the data and search time?

See retrieving data is not an easy because your RAM memory area itself will be very costly, you can think about how many G B in ram may be 8 G B, 16 G B, 32 GB. But he is talking about 10 to the power 10 or some size of database. So, page fold will be increased all sort of things will be there. So ultimately you have to think about these 3 terms one is classification, another one is clustering and another one is indexing.

Now, what is the difference between the classifications and cluster? Any idea? The terms you have heard.

(( ))

And classification also divides group

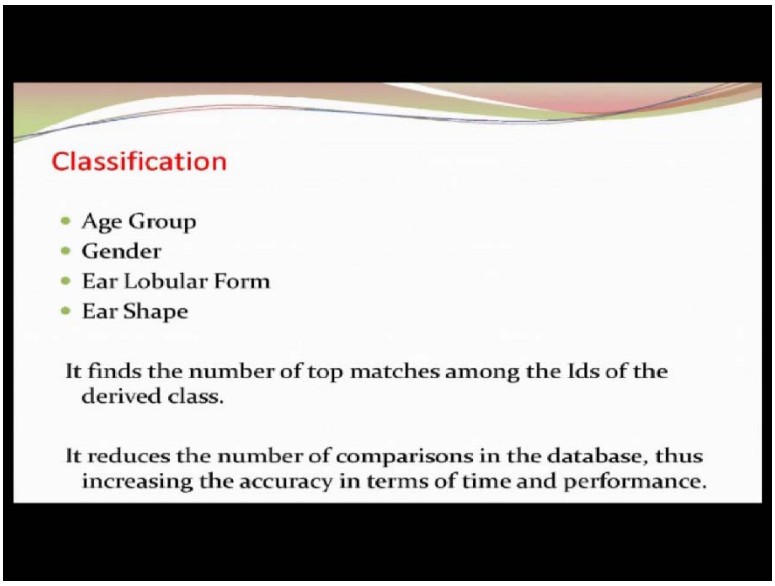
Supervised and unsupervised.

One is supervised, another is unsupervised. The classification is based on your idea say, male female or the different age groups or may be that ear shape, height, width like that you can think some of them are fixed, some of them are not fixed. So, weight is variable, age is variable so you cannot consider perfectly this. Clustering is based on your characteristics based on your characteristics means, say feature points you have the feature points, based on the feature points you want to cluster them.

So, there are several clustering techniques exists like Kevin(s) clustering techniques, fuzzy clustering techniques and Kevin(s) is the best known clustering technique provided that you know the value of k. How many clusters you have to make? In reality, in the case of biometric system if I know the value of k, then I have solved several things this is not known. Second thing is that think about this finger print which is 1 inch by 1 inch, there are 100 points and there there must be some points they are very closely associated.

How can you cluster them? So these are also big issue and classification if I make it as gender based then you are reducing by half. Say, I have a 100 crore people reducing by half also another crore people, 100 into 50 crore search will not be that much effective. Indexing is another one where we can spend time. We can do something that you arrange the data in such a way that get a data then, you try to get a proper index for that query image and go to that searching area. So can you index a data in such a way that the index data will be in some order. So that searching time will be reduced so, we are not spending much time towards this one we are spending time to this one.

(Refer Slide Time: 34:47)



Classification

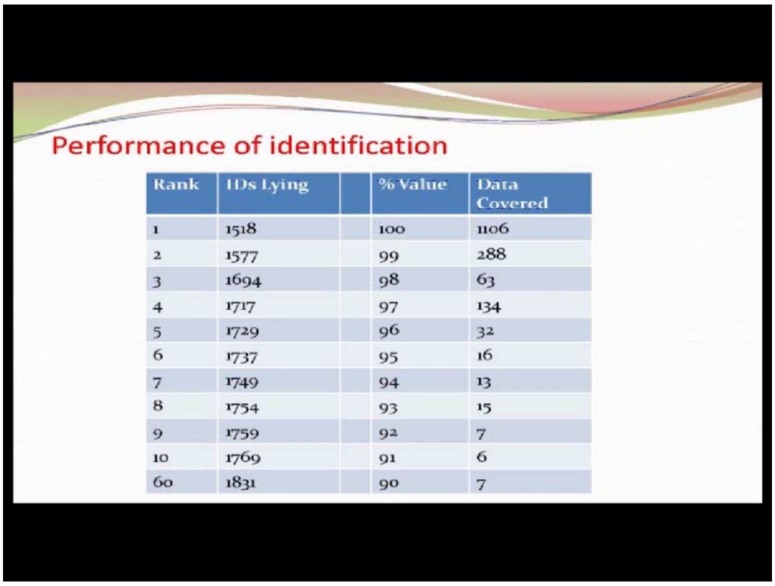
- Age Group
- Gender
- Ear Lobular Form
- Ear Shape

It finds the number of top matches among the Ids of the derived class.

It reduces the number of comparisons in the database, thus increasing the accuracy in terms of time and performance.

So, classification I told you the age group can be considered middle age group, young age group based on date of birth you can think. Gender is one, ear lobular form this smaller part that is everybody has different type. But not too many sizes 6 size types of things, then ear shape, triangular, oval like that shapes are there that is 4 or 5 shapes. So, these can be considered for classifications.

(Refer Slide Time: 35:23)



Performance of identification

Rank	IDs Lying		% Value	Data Covered
1	1518		100	1106
2	1577		99	288
3	1694		98	63
4	1717		97	134
5	1729		96	32
6	1737		95	16
7	1749		94	13
8	1754		93	15
9	1759		92	7
10	1769		91	6
60	1831		90	7

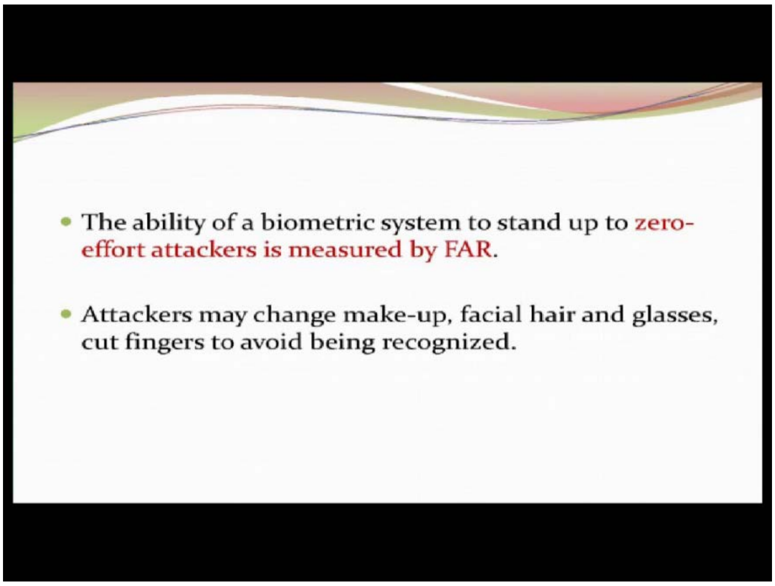
Whatever results we have obtained that also I should tell we have the database of roughly 2000 but top one, best match 1518 of them having the rank 1 and the coverage is 1106 data covered. So rank 60 is very poor but the result is that 1831 data is lying in that and data covered is 7 only. So this is the performance, moderately good performance that is the reason why I am telling that our performance is not that bad except that database size is less.

See, I am looking for rank 1 top 1 rank. So, I got that rank 1 out of that 1518 cases and data data covered means that how much data I have covered? There are term called as penetration rate and heat rate so, those terms will be cover in the identification. So data coverage is 1106 here 60 percent rank [FL] means rank 60. Because I am telling that my data is laying in the top 60 I am happy the police department they never tell that I want the best match, I want that moderately reduced size and my search zone will be less, then I will do another method to pick them.

What they do basically? Suppose I understand that crime has occurred then in that locality say 10000 people are there. So, all of them are not not performing the same crime so, based on the crime effect they bring up the search search area very small then they do the other method to obtain who has committed the crime?

Same thing, if get the top 1 rank matched, that means he is the best match he is the person directly I am telling. And, top rank 60 means that my person is lying in the top 60. One of them it may be first rank, it may be second rank it may be sixtieth rank. So that is the idea. Then what for we are thinking about identity? See, I am looking for proving my identity so, there must be some attacker who wants to prove himself as a same identity or he does not want to prove himself the same identity, this is one of the thing is true.

(Refer Slide Time: 38:33)

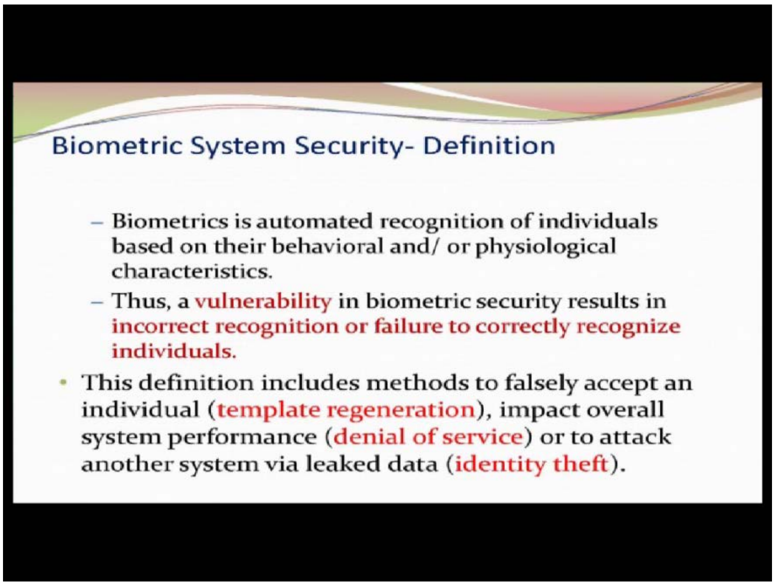


- The ability of a biometric system to stand up to zero-effort attackers is measured by FAR.
- Attackers may change make-up, facial hair and glasses, cut fingers to avoid being recognized.

So otherwise, why one should test what is identity if all can be trusted. So, what is our aim? The ability of a biometric system to stand up to the zero effect attackers is measured by false acceptance rate that is 0 level attack. Means your false acceptance rate should be 0. This F A R you want to make it 0 so, that there is no false attack.

So, this false attack can come in different way in the case of face facial recognition or facial system I can come with the makeup or extra hair or glasses, in the case of finger prints I can cut my fingers and so on. So different level because these are all hostiles one but this can occur in the case of biometric system.

(Refer Slide Time: 39:16)



Biometric System Security- Definition

- Biometrics is automated recognition of individuals based on their behavioral and/ or physiological characteristics.
- Thus, a vulnerability in biometric security results in incorrect recognition or failure to correctly recognize individuals.
- This definition includes methods to falsely accept an individual (template regeneration), impact overall system performance (denial of service) or to attack another system via leaked data (identity theft).

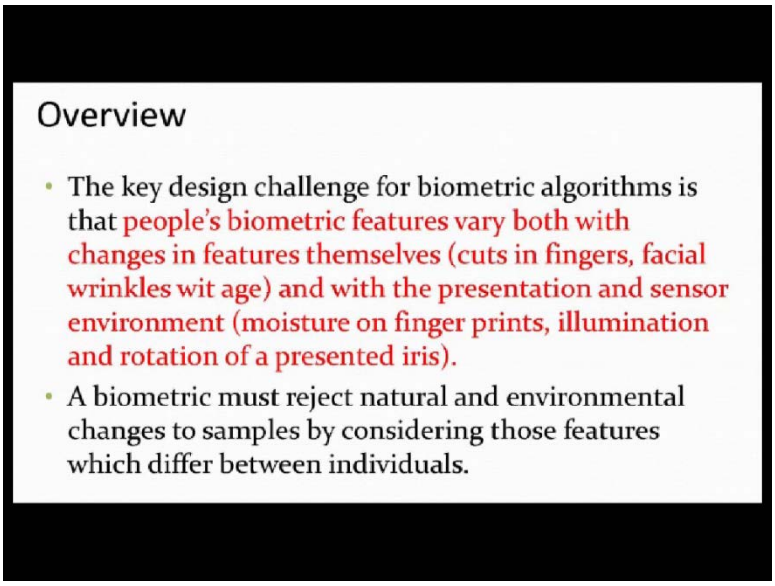
So ultimately, if you see carefully this is nothing but behavioral physiological characteristics that is the things you consider for biometrics trait. And, your vulnerability in the biometric security results either incorrect recognition or failure to recognize correctly. Either it will be incorrectly recognized, falsely accepted or failure to recognize individuals correctly that means, these are the two ways that a false acceptance and false rejection rate has come.

Now, these definitions include the methods to falsely accept an individual. Which is nothing but the template of feature regeneration, that what I will be doing? I will be generating the features for you and falsely accepted. This is possible, attacker will be doing that one, then impact overall performance. This is another parameter that I am an attacker; I want to show that your system is poor. So, that the organizer will change your system by another system and that system is salable, that system is under my control. It may so happen right so impact overall system performance.

Then denial of service, so that is the thing I am telling that suppose you have a system and I am an attacker, I will try to prove that your system is bad that means I have increased false rejection rate by some method. So every genuine user will be out, they will be told that no, you are not a user. So inconvenience will be high and then the organization will think that this system is no good I want to change it so that is possible.

To attack another system via leak data and also through this system suppose I have logged in and I could make the access control then I can go to the other system and spoil that one, that is also possible. So, identity theft is coming in between so, this attacker has a major role to play to spoil your system in different ways.

(Refer Slide Time: 41:46)



Overview

- The key design challenge for biometric algorithms is that people's biometric features vary both with changes in features themselves (cuts in fingers, facial wrinkles wit age) and with the presentation and sensor environment (moisture on finger prints, illumination and rotation of a presented iris).
- A biometric must reject natural and environmental changes to samples by considering those features which differ between individuals.

So what is the challenge in biometrics algorithms? The people(s) biometric features vary both with changes in features themselves cut in fingers, facial wrinkles etcetera. Based on that, there will be change in your features. And also, with the presentation and sensor environment, the way you are presenting your data sometimes, you will like to make the system full by putting the 50 percent of finger print or like this and you test whether I am been accepted or not? Sometimes, due to the weather atmosphere that, temperature is very high or your humidity condition is very high so, that that may affect the use.

So with the presentation sensor environment you may be giving the different type of feature vectors. Say, biometric system must reject natural and environmental change that is your first part. The natural change means that your face gets changed after 5 years or 10 years, system must be robust against that. System must be robust against the any change due to the environment. Atmospheric condition is poor so, system should not stop you, should not throw you out that you are not matched, because if if you are throwing out that, that type of cases then the chances of false acceptance and false rejection rate would be high. So the attacker will get an opportunity to enter into your system.