Biometrics Overview (23-24 - Update v2 Oct2023)

Welcome back. In this video, we're going to be introducing biometrics. It's very likely that you've come across these in your day to day life. Many phones and modern devices come with inbuilt fingerprint recognition or even facial recognition, so this shouldn't be a new concept to you, but we will break it down a little bit more.

To start off with, biometric is a sufficiently distinct trait which can be measured, quantified, and stored in such a way as to allow authentication to happen for the end user. We can split it into two different categories, physical biometrics, such as facial identification, fingerprint recognition, and so forth, versus behavioural biometrics, which are things like how you type. There are two stages when we look at using biometric authentication. There's enrolment and then the operation.

When we look at enrolment, what we're trying to establish is what's referred to as a template. A template is basically the computer representation of that distinctive trait. So for example, a fingerprint could be broken down into aspects, such as the swirls and loops within your fingerprint. Having this template stored means that when you go to authenticate, you provide your biometric, and it can take that, perform the similar calculation, and determine whether it's sufficiently close to the template. This brings us on to the different modes of operation.

Within biometrics, we can either use it in identification mode or verification mode. Verification mode is very likely what you use most of the time. This is where there's a template stored, you've already claimed your identity, and you're just trying to check that the biometric you provide matches the identity template that they have on the database.

In contrast, identification mode is more like what we would think of as a watch list for the FBI, where you're presented with a biometric and you need try and find the corresponding identity from the database. That's a much more challenging problem and not one that we are particularly interested in for this module. So, we'll focus on verification mode.

When looking at different biometric systems, one helpful tool is to be able to determine whether one is better than the other. In order to do this, we need to define a few metrics, which are going to be helpful. We have true positive, true negative, false positive, and false negative. A true positive is where someone is the genuine user and is accepted as they should be.

A true negative is where someone isn't a user and they are correctly rejected. A false positive is where someone shouldn't be allowed access, but is allowed access. And a false negative is where someone should be accepted, but they have been rejected. Clearly, in any biometric system, we want to maximise the true positives and minimise the false negatives.

This can be a real challenge. One way of modelling this information is to use an ROC curve. We'll take a look at what that looks like now. If we want to determine the effectiveness of biometric system, then one tool that we have at our disposal is a ROC curve or ROC curve for short. This stands for Receiver Operating Characteristic and this doesn't really help us in terms of understanding what it is. So effectively, you can ignore that, and just refer to it as an ROC or ROC curve. Effectively, what this does is it maps our true accept rate, so that's the proportion of people who were accepted and should have been accepted versus the false accept rate. So that's the proportion of people who were accepted, but shouldn't have been.

We can calculate these values by the following. Our true accept rate is going to be our true positives versus true positives plus false negatives. So true positives and false negatives is the total number of actual positives that we should have. And similarly, we've got our false accept rate, is equal to false positives divided by false positives plus true negatives. And the number in the bottom here is all the possible negatives that we should have, so the total of the true negatives plus those that we misclassified as positive.

We can map the value for a given biometric classifier on this graph shown here. On the x-axis, we have the false accept rate. And on the y-axis, we have the true accept rate. At the corner, we have the value 0, and our maximum is going to be 1 on both of these as we are working with a proportion of the whole.

Now, when we look at our classifier effectively, what you're going to end up with is a score. You're going to look at the biometric that's provided. You're going to perform whatever transformations and calculations you need to complete, and then you need to make a judgementÂ as to whether you accept that it matches the template or doesn't match the template. Now, this is normally done on a sliding scale.

So on this sliding scale, we need to decide, at some point, at which point we'll say, OK, this is where we're going to accept that these two are similar enough in order to provide a positive result. Now clearly, this threshold can be moved around. You can say move this closer to zero. In which case, you're going to get more true positives because you're catching more people and saying that they're positive, but you are also going to increase your false positives because you're lowering that threshold for acceptance.

In contrast, if you were to move this higher up, then you would get certainly lower false positives, because you have a higher standard to meet. However, you would also get lower true positives. You'll start to reject people who should be accepted. So it is a bit of a balance trying to find out where on that scale we want to place our threshold.

On our ROC curve, if we were to take a particular biometric classifier or biometric system and plot the true accept rate and the false accept rate for all the different thresholds that we wish to look at, then we can make our ROC curve. Now, if we were to do something and it was basically random guessing, what we would end up with is a diagonal line up here. Then for our curve, if we start off at 0, then we'll end up with something which looks a little bit like this, where that's going to end up as 1 comma 1. This means that we can start to compare different systems because we can have curves which look a little more like that, or, indeed, a little more like this.

Now, ignore my poor drawing skills. If you consider the three curves that we have here, I'd like you to take a minute to think instinctively what is the better system here. Well, the better system is the one that gives us a better true accept rate and a lower false accept rate. In this particular instance, this curve at the top here is performing better. We're getting a higher true acceptance rate for not much of an increase along our false accept rate.

Whereas, this bottom curve, there's not terribly much movement there. It started to become closer to guesswork. Now clearly, there's a lot more that can be said about our ROC curves. But for our purpose, this is sufficient. We've now covered the fundamental building blocks of biometric authentication. I hope you've enjoyed the video, and I'll see you next time.