Further Biometrics - part 1

Welcome back. In this video, we're going to take a slightly more in-depth look at some common physical biometrics as well as a high-level overview of behavioural biometrics. Biometrics offer the benefit of less cognitive load on the end user. You don't need to remember a range of passwords or other knowledge-based authentication.

Instead, it's something which comes inherently with them, such as a fingerprint or an iris or retina scan. In this video, we'll take a little bit of a deeper look into fingerprints and iris and retina scans. However, biometrics is obviously a field in its own right. As a result, you can go very in-depth into these areas. So what we'll focus on today is a high-level level overview of how these different methodologies function, starting off with facial recognition.

It's likely that you may have had some experience of using facial recognition by yourself. Whilst technology is certainly improving in this area, it's still by no means perfect. Recall that we have two possible uses or modes of operations with biometrics. We've either got identification, where you have a range of possible images and you're trying to identify an individual person within that.

Or the verification, which is what we are focusing on, where there's a stored biometric, perhaps in a device, such as a mobile phone or tablet and you're just trying to verify that the identity claimed matches the one stored. With facial recognition, we're commonly looking at aspects such as features on the face like the distance between your eyes, the length of your nose, distance between the mouth and eyes, a variety of different focus points on the face. This can then be translated into a template when you are registering. Then, when you go to authenticate, it tries to extract this information again from the visual that it has and sees whether it closely matches the template stored in your database.

There are a range of different options in terms of the algorithm used to implement this. One such algorithm as to use Eigenfaces. However, there are a variety of different algorithms out there. The NIST does regular testing of a range of different mechanisms, looking at aspects such as how effective the false accept rates and false reject rates are, and so forth.

So there's a lot of data in that kind of field. One interesting area of facial recognition is around the diversity of the faces used to train such systems and algorithms. There has been a lot of research done at MIT which demonstrated that facial recognition was inherently biased, particularly towards white males.

So it's clearly a field which has a lot of different facets and it's good to see that we've been moving forward in this area. There is, obviously, the privacy issues and we'll come back to speak a little bit about those later in the video. Real-world world use of facial recognition can be a little bit patchy. In particular, you've probably seen a number of news reports related to the use of facial recognition in crime settings and how individuals can be falsely registered as criminals. So clearly, there's a few things to consider there.

It's also quite possible that in using facial recognition, you get a lot of false rejects. So as we improve, it's important to keep a balanced view on the benefits and the drawbacks of using such a system. Let's now move on to iris recognition. The iris is effectively the colour around your pupil.

The patterns in this, if you look closely, are very unique. So much so, the iris recognition is seen as one of the most reliable biometrics that you can use. Even individuals who may be genetically linked, such as identical twins, are going to have sufficiently distinct iris patterns. For enrolment in iris recognition, a near infrared or infrared camera can be used to take an image of the eye. The image is then examined with an algorithm to calculate coordinates for the pattern.

A template is then formed. At the time of verification, another image is taken. The software is going to extract the features from that image and determine whether it meets the threshold when compared to the template. Another option when we are looking at the eye is a retinal scan. These are, effectively, the blood vessels at the very back of your eye, behind the lens. When light is shone onto those, they light up in a different kind of pattern, and so that information can be used to uniquely identify an end user. This is often thought as the pinnacle of physical biometrics, it is highly accurate.

However, the retina can change with disease or age, so there's always the potential downfall of that changing. Another issue to consider with retinal scanning is that it's generally considered more invasive than iris recognition, and as a result, this means that the end user may be less likely to use it. It can be used specifically in particularly high security situations where the cost of hardware and the invasiveness is not perceived as a particularly important constraint. Let's move on to the fingerprint.

This is probably one that you use on a daily basis. Many modern devices use a fingerprint sensor in order to unlock and lock them. When you look at your fingerprint, you will notice that there are what is referred to as ridges. Effectively, these are the lines on your finger. You

will also notice valleys. This is the space between the ridges.

These from a range of shapes and patterns, which can be referred to as minutiae. Let's have a look at what's modern minutiae for fingerprints look like. On screen here, you can see a number of different patterns which can be used in fingerprint recognition. The top three basic patterns are what was traditionally used within fingerprint recognition. However, we've now progressed within the field and use what is referred to as minutiae patterns.

Here, we have patterns such as ridge endings, where a line stops or dots, where there's a small ridge within two larger, bifurcations, where a ridge splits into two, trifurcations, where it splits into three, and a variety of other options, as shown here. Notice how the new patterns are providing much more complexity in terms of the detail. This provides more features to be extracted for templates.

That's us video where we've had a look at facial recognition, iris scans, and also retinal scans. I hope you enjoyed the video, and I'll see you next time.