Introduction

Security is a big concern for people and companies in all fields; for we all have secrets to keep. However, in order to do that we need reliable systems in place. Systems that can protect our stuff from malicious attackers.

Biometric Authentication is name for the category of systems that protect our secrets using information we keep on ourselves – our bodies. The specific pieces of our bodies used for the authentication are called modalities. Here we will talk about the face modality (Facial Authentication).
Facial Authentication relies on scanning a person's face for facial contours, pores, and other facial characteristics that make a person's face unique.

**Anti-Spoofing**

Facial Authentication is in practice a very effective way to differentiate between attackers called imposters and genuine users. However, there's a problem. Any field dedicated to securing something also included the study of methods to break that security.

In Biometric Authentication for any modality this is called ‘Spoofing’. When a system is spoofed it has been deliberately made to allow an imposter in. There is a constant arms race between those who make the systems secure and those who break. However, people can be easy for the study of ‘Anti-Spoofing’ is all about deflecting these spoofing attacks. Below, there are three ways that Facial Authentication systems are kept safe from attackers.

1) **Challenge Response strategies**

For Facial Authentication to happen you need a sensor which will take a photo of you face to compare against saved photos. From this an obvious spoof arises, tricking the sensor using an existing photo of the genuine user. After all, due to the Internet photos of most people can be found all over social media. To overcome this ‘Liveness Detection’ is implemented; detection that the subject is alive i.e. not a photo.

There are ways to combat this. One way is to have the sensor look for movements like eye-blinks and gaze changes these are called ‘Challenge Response strategies’. These little things are highly effective against photo attacks, but sometimes the imposter will use a video which has all these things. To combat video based spoofs, there are a fair amount of techniques. They are fairly complex but can generally summed up as looking for cues that the information presented to the sensor is not a video by looking at things that a video on a screen produce, or try to take in information from the surroundings that would show the sensor there was no live human in front of it.
2) **Sensor Modifications**

As described in the last point, the most common form of attack against facial recognition is a video or photo being provided to the sensor. There are a few ways which the sensor itself can be improved without changing the software.

One simple way is to add inferred information to saved genuine information. Humans radiate heat that can be seen with an infrared camera and cannot be easily shown on a video. Moreover even if the imposter naturally looks very close to the genuine user like a twin, this has been shown in [1] to still be effective. Another way is to add lights in a certain arrangement to the sensor. Since a video will be played on a screen it will be reflective, the lights can simply make it very hard to detect anything if a screen is placed in front of it.

3) **Using multiple biometrics**

As simple to way to improve the effectiveness of facial Authentication is simply to use more than one modality. Supplement the reading of facial information with say fingerprint or iris modalities or even voice. This does not completely mitigate the dangers spoofing but certainly raises the bar considerably for an imposter to gain access.

**Overall**

Facial recognition is a very good form of Authentication, but it still has problems. Problems which come in the form of attacks from imposters, to that tend anti spoofing is there to save it. Regretfully, anti-spoofing does not always work.

There are problems with each of the methods. Challenge Response methods are the best for the device since the sensors do not need to be changed, but have the problem of becoming increasingly complex with time. Checking for blinks and movements slows down the recognition time, and anti-spoofing against videos requires computationally intensive math which drains the battery. Their advantage is also just that, they can be improved without
needing to get a new device. These sort of improvements also fail when the imposters get even better spoofing attacks.

Sensor modification is not very good for an user wallet. Adding any sort of modifications to the device requires money and a new device, but is a better choice long term. Because it sets a much higher bar for an imposter to begin to attack the device. The device as well suffers because of added battery consumption, but everything else should stay the same.

Lastly using multiple biometric would yield the best security at the worst price. It would require a new phone with extensive modifications to allow for a new sensor to be integrated which would be paid for by the users in money and by the device in accommodating all the extra computations and resources needed for it. And like a sensor modification it can still fail as it comes with its own weaknesses like facial recognition does, but sets the bar much higher for an imposter to begin attacking the device.

**The Future**

No security system is perfect: Biometric Authentication or not. But, we can work towards making a system that is really secure. To that end, Biometric Authentication is far more secure than simple password or pin for unlocking things. Yet, the still do make mistakes. From the research, the future direction of Facial recognition seems to be going towards better sensors and combinations with other sensors in terms of newest growth, but most of the research has up to now been focused on improvement using software.
References

Images

1. Figure 1, From Research article [1], page 1532
2. Picture of Nodal points from The NEW ECONOMY
3. Figure 2, From Research article [1], page 1533
4. Picture of phone unlocking device from DroidViews

Research Articles

   doi: 10.1109/ACCESS.2014.2381273
   URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6990726&isnumber=6705689