Practical 8 – Presentation Attacks on Fingerprint/Face Capture Devices

Ole André Hauge

March 21, 2021

Presentation Attacks

1. We discussed the fundamentals of presentation attacks.

   (a) [3 points] What kind of innovative attacks can be used to defeat the face biometric systems other than printed and electronic attacks? Comment on ease of artefact costs in various cases.

   Answer: Several different attacks can be used to defeat face biometric systems. An attacker can use morphing, a technique where images of different people are merged in such a way that the attacker can be identified as another (or more) person(s). This can be used to defeat passport checks where the images are used to authenticate the owner. This technique, that being the morphing of the images does not need to cost that much, although creating a fake passport might be a bit costly.

   Another technique can be, as mentioned by Christoph, 3d masks, either made of silicone or simpler 3d printed material. These artifacts vary in price but everything from 100USD (simpler 3d prints) - 3000USD+ (silicone) is to be expected.

   A simpler method could be to use makeup to be identified as another reference or to conceal ones own identity to evade detection if one is running from law enforcement. These artifacts do not have to be costly as one can use makeup and change the hairstyle to something more "artistical" which covers part of one's face.

   (b) [3 points] Iris recognition systems are considered for robust applications. Can they be attacked with different presentation modes? Briefly comment on different attack types for iris systems.

   Answer: Yes they can be attacked. One may present a print-out image or recorded video of an iris in hopes of defeating the system, although methods are now in place to make this harder e.g. heat detection, NIR sensors to see the iris's vein-structures, and more.

   In more advanced techniques, if the attacker has access to the actual iris e.g. an iris image, the attacker could make fake textured contact lenses or even make synthetic irises. A more morbid option could be to use "post-mortem" samples from dead subjects or just stealing an eye. Although these attacks demand artifacts that either are more costly or harder to acquire, like an actual eye of a dead person.

Presentation Attack Detection

2. We discussed the fundamentals of presentation attack detection.

   (a) [2 points] What kind of simple liveness detection can be used to detect presentation attacks in a video based face recognition system in visible spectrum? Are they robust always?

Answer: Simple methods could be to instruct the capture subject to conduct specific movements e.g. nodding or blinking, although this might be defeated by recordings it will eliminate simple printing and electronic image attacks.

Further, using pre-trained SVM (or similar models) to evaluate the probe can be a fairly simple way of detecting liveliness as long as the models are trained using a sufficiently large training dataset. The weakness with these kinds of detectors is that they are trained on a specific kind of data, in this case, presentation attack, thus other types of attacks might not be detected by the detector as the model has no idea of how these will/should be detected. It is not possible to train for every possible attack type as some are unknown to us. The attackers are always developing new ways of defeating the security measures, thus fueling the continuous "cat and mouse" game that is the information security field.

(b) [2 points] In our earlier lectures, multi-spectral, and hyper-spectral cameras were discussed for face recognition systems. Can you comment on the suitability of such cameras against electronic attacks?

Answer: The use of such cameras can be a simple way, perhaps a bit costly depending on how it has to be implemented in the pre-existing solution, to hinder electronic attacks as it can capture an image of the presented probe in greater detail by seeing light in different bands at the same time. By enabling the use of for example NIR and normal spectrum imaging, we would for example prove that the electronic sample did not have veins and thus was an imposter. In short, this technology enables a greater depth understanding of the presented probe and can be used to identify details that only can be present in actual living probes.