CSE 40537/60537 Biometrics - Spring 2020
Instructor: Daniel Moreira (dhenriq1@nd.edu)
Final Exam

[Question 1]

Imagine that you were hired by a major hospital chain to coordinate the deployment of an access management system to control the entrance of nurses and physicians into their controlled drug storage rooms. The manager of the hospitals has heard about Biometrics but is not certain about the benefits of using it. She believes using a simple access card and numeric password is as effective as using a Biometric system. It is your duty to change her mind. What would you say to convince her?

[Random Good Answer]

So I want to convince you from two different aspects, convenience and security. And those are the main benefits for using Biometrics. We want the system to be convenient for physicians and nurses to use and also the controlled drug storage rooms need to be secured to prevent other people getting into it. For convenience, our target users do not need to bring any access cards and they do not need to remember the passwords. So they can go to storage rooms at any time they want and do not need to consider if they bring the card with them or not. Also, biometrics is safer. As the manager of the hospital, you cannot control everyone in the hospital. If some physicians or nurses lend their card to other people that do not have access to the storage rooms and also tell them the password, then lots of people can get into those rooms which makes the hospital really hard to control those drugs. This thing might happen even if the physicians or nurses do not have time at that moment and they want their assistants to help them. But with a biometrics system, they must go to the storage room by themselves. And there is about no risk that the access key will leak to other people.

[Questions 2 and 3]

Good job, you have convinced the manager to adopt a Biometric system! Now, taking into consideration the characteristics of COVID-19 and the Personal Protection Equipments (PPEs) one needs to protect against it[1], answer the following questions:

[Question 2]

What Biometric **traits** and **sensors** would you **avoid** using in the system? Please explain why, taking into consideration the usage and removal of PPEs, as well as any of the concepts of universality, uniqueness, permanence, measurability, acceptability, circumvention, accountability, and performance, if relevant and applicable. Please analyze **at least two** combinations of trait and sensor.

[1] https://www.cdc.gov/coronavirus/2019-ncov/downloads/COVID-19-PPE.pdf

[Random Good Answer]

The first system trait combination that I HIGHLY suggest be avoided is any combination of online fingerprint acquisition with a device that requires physical contact in which one is required to make contact. Given that we know COVID-19 can be transmitted through surfaces that have come into contact with the virus it would seem irresponsible to promote physical contact with any surface unless required and even then it should be with the use of gloves which would make it impossible to use fingerprint recognition. A possibility may be to use the types of fingerprint acquisitions that use 3D imaging and does not require physical contact, but given that one has to be near and may make accidental physical contact along with the widespread use of gloves, this also seems like a poor idea.

Another combination that I would suggest be avoided is the usual manner of facial recognition in which a camera detects a person's face and compares it with the template database. In trying to deal with COVID19 the use of facemasks has become prevalent and asking someone to take their mask off might mean putting them at risk of infection. Since masks obstruct most of the lower part of the face it is reasonable to assume that facial detection would just not work as well as intended.

[Question 3]

What Biometric **traits** and **sensors** would you **recommend** using in the system? Similar to question 2, please explain why. Please analyze **at least two** combinations of trait and sensor.

[Random Good Answer]

I think the ideal system in this case may be some sort of iris detection system in which one can be reasonably far away from a camera while still using any of the PPEs that they may have. One good example could be those existent in Schiphol airport in which one can be about half a foot away and not take off their PPEs.

One other good possible trait that could be checked is actually voice recognition, one can be fairly far away from any system and still manage to have the voice heard. One worry for me about using such a thing is that masks could make the sound that you produce become muffled and in those cases it may not be the ideal choice. Given that voice can be affected by factors like being muffled or even being sick or having a sore throat, I believe that the most ideal is still iris recognition.

[Questions 4 and 5]

Good job, the manager was convinced by your recommendations! However, she has just told you that the hospital chain is, unfortunately, facing a financial struggle and that most of the funds had to be spent with ventilators. Hence, she has decided to reuse an off-the-shelf fingerprint recognition system that was bought in the past to sign in patients in the front desks. She has explained to you that it might work since controlled drug storage rooms rest outside intensive care units, where facial masks are the only required PPE. In addition, hand sanitizers are available on the doors of every room. She has taken full responsibility for this decision and it is now your job to help her make it work.

[Question 4]

While reading the system specs, you have learned that the software performs **identity verification**; it requires swiping an insurance card besides the fingerprint presentation. What are the **pros** and **cons** of turning this system into an **identification** one?

[Random Good Answer]

Pros:

1. The identification doesn't require the user to input their identity. Hence, the user doesn't need to swipe the insurance card anymore.

Cons:

1. The identification will take more time than verification, as it needs to match the user's feature with all other subjects in the dataset.

2. The identification system tends to make more errors. If the user has similar features with more than one subject in the system, there might be wrong results.

[Question 5]

After getting to know the differences between verification and identification systems, the manager has decided to endorse an identification set-up. To adapt the old system, the lead developer of your team has come up with the following solution: wrap-up the fingerprint matching routine in a loop and compare an eventually acquired fingerprint with every fingerprint template enrolled in the system database. The chosen identity should be taken as the one whose template presents the largest similarity score with the acquired fingerprint. What is the major flaw in this solution? How would you fix it?

[Random Good Answer]

The major flaw in this system is that there is no guarantee that the fingerprint presented to the system is enrolled in the system. In essence, this system would not be a security system as every fingerprint presented would be identified as someone enrolled in the system. The fix to this would be to establish some sort of threshold; a match must achieve at least a certain similarity score to be considered a true identification, so that not every fingerprint presented would have a match.

[Questions 6, 7, and 8]

While reading the specs, you have also learned that the system uses a single finger USB optical sensor, whose resolution is equal to 1200 ppi. The documentation says the software relies on level-2 features, and when running in debug mode, the sensor has a small embedded display that shows a float similarity score for each event of fingerprint presentation. Given this information, please answer the following questions:

[Question 6]

What are fingerprint level-2 features? How are they related to Galton’s details?

[Random Good Answer]

Galton's details include bifurcation, ridge endings, and dots or islands of the fingerprints. The fingerprint level-2 features are minutiae (Galton’s details), where ridge endings and ridge bifurcation are mostly used.

[Question 7]

In your opinion, how easy would it be to perform a presentation attack on this system? How would you prevent it, keeping the same sensor but adding extra modules of software?

[Random Good Answer]

In my opinion, this system might be really hard to attack. The desired resolution for a level-2 feature identification is 500 ppi, while this system has a resolution of 1200 ppi. On the other hand, as we saw in class, level-2 features can be reproduced. Thus, one would be able to create fingerprints and attack the system. To fix this issue, I would add/change a layer of software and analyze level-3 features. The desired resolution would be at least 1000 ppi and our hardware is above that; thus, we could detect liveness by analyzing sweat pores and lifetime acquired marks.

[Question 8]

How problematic would it be to deploy the system in the production environment and let it run in debug mode? How would you exploit the exposed similarity scores to attack the system?

[Random Good Answer]

In the production environment, the users will be able to see the similarity scores visible in the debug mode and based on the acceptance and declination, they can estimate the threshold value for the system which is confidential information for the security of the sensor. I can perform an indirect attack on the system taking advantage of the score to iteratively change a synthetically created template until the similarity scores exceed a fixed threshold and grants access to the system. This attack method uses a variant of hill climbing algorithm.

[Questions 9, and 10]

So far, the hospital manager is happy with the prospects of the Biometric system to be deployed. Nevertheless, you know you did not try yet the use of **multibiometrics** to increase the security and the final performance of the system.

[Question 9]

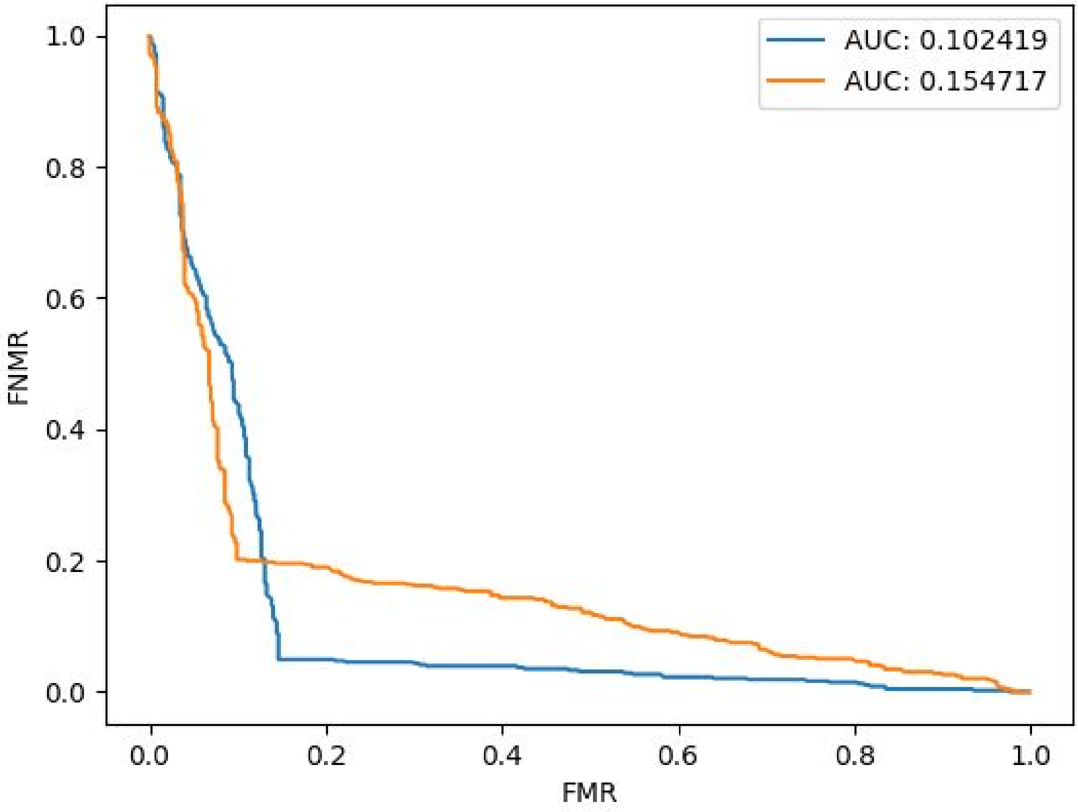
What multibiometrics strategy would you adopt to increase the fingerprint system performance at hand with nearly no additional operational cost (no need for extra sensors or extra software modules but only an affordable increase in runtime and in template database storage)?

[Random Good Answer]

The simplest and quickest way to implement multibiometrics would be to make the system require multiple instances. By requiring the user to present multiple fingerprints there would be no need for additional sensors or software.

[Question 10]

The lead developer of your team was able to generate the following graph with the performance of the system before and after the use of multibiometrics, at the cost of doubling both the runtime (from 5 to 10 sec) and the template database size (from 100 to 200 MB). What is this graph showing? Should you keep or discard the system modification? Please explain as you would do to convince the hospital manager.



Graph 1 - Orange: System behavior with no multibiometrics. Blue: System behavior with multibiometrics.

[Random Good Answer]

The graph is showing the ROC curves for the different system states. The FNMR and FMRs at different thresholds are plotted. They will tell you the best solution by using the smallest area underneath each curve (the AUC). So, in this graph, the lowest AUC would be the blue, the system behavior with multibiometrics. Then, it is best to keep the system medication. I would try to explain to the hospital manager that the AUC is telling us which system version has the lowest total false positives and false negatives at various thresholds, so no matter where the cutoff is, the system likely guesses accurately more often than not. The use of multibiometrics in the second system creates improvement without any additional cost of new sensors, modules. For a sensor that is simpler, greater accuracy would be very beneficial, as we cannot use other elements that other sensors can capture.