CSE 40537/60537 Biometrics - Spring 2022
Instructor: Daniel Moreira (dhenriq1@nd.edu)

Student (Printed): _____ **(Signature):** _____

Midterm Exam - 03/04/2022

[Question 1] (2 points)
Suppose you were hired by a bank company to coordinate the deployment of an access management system to control the entrance of authorized people into the many vaults spread among different branches. The bank directors have heard about Biometrics but are not certain about the benefits of using it. They think using simple access cards and long passwords is as effective and much cheaper than using a biometric system. If it is your duty to change their mind, **what would you say to convince them**?

Using biometrics would be a much safer system, since it uses a physical or chemical trait, rather than something that can be stolen as easily as an access card. A password could also be given to somebody else or bruteforce searched to produce attacks. Furthermore, it would be more convenient for the authorized people, as forgetting a long password or losing an access card would not be a problem. (Biometrics uses a trait you always have on you). Also, problems like typos, and card damages are more likely to happen than losing a fingerprint, iris, or face.

[Question 2] (2 points)
One of the bank directors is worried that he has an identical twin. He claims his brother will also be able to enter the vaults in case he is enrolled in the biometric-based access management system. Is he correct? **What traits would you recommend** the adoption considering his concern? Please justify your answer.

If the twins are identical, so they have exact same DNA. However, same DNA doesn't mean they have exactly same biometric traits such as faces, fingerprints, and irises. In one sense he is wrong. However, on the other sense he is slightly right if the biometric system consider ~~DNA~~ faces. Sometimes, study showed that twin may have same faces in this case the manegen is right. The manager will be 100% right if they use DNA sequence for identification and verification. 2.0

To make the enrollment system more robust for twin I would recommend fingerprint and irises recognition system. Because twin dont have same iris and fingerprint pattern. These traits are unique for identical twin.

[Question 3] (2 points)
Another bank director is worried about the pandemics, the spread of germs, and the need for the use of masks. Taking his concerns into consideration, **what biometric traits and sensors would you avoid** using in the system? Please explain why, taking into consideration the characteristics of the pandemics (it spreads when an infected person breathes out droplets containing the virus), the usage of masks, as well as any of the concepts of universality, uniqueness, permanence, measurability, acceptability, circumvention, and accountability, if relevant and applicable. Please analyze **at least two** combinations of trait and sensor.

One combination of trait and sensor that I would avoid would be fingerprints with a pressure sensor. There is a good chance that germs will be spread if the bank is using a sensor that people are constantly touching right after each other. Everyone touching the same surface to measure their fingerprints could be a good way to spread germs. A second combination would be faces and a facial scanner. The fact that everyone is wearing a mask due to the pandemic and covering up half of their face would make it difficult for a facial scanner to be accurate. People could pull down their mask for the scan, but that might not be as accepted and makes measurability more difficult.

[Question 4] (2 points)
What biometric traits and sensors would you recommend using in the system, considering the same concerns? Similar to question 3, please explain why. Please analyze **at least two** combinations of trait and sensor.

of trait and sensor. ✓fingerprint

① 3D Imaging Touchless sensors: No need to take off mask, much more sanitary, fingerprints are nearly universal & very unique more sanitary because no surfaces are touched. This system is also robust because it cannot be fooled by flat paper images of a fingerprint; easier measurability → people just present hand

② Deformable cameras for iris recognition: this system can be employed from 1.5m - 2.5m away from subject, could facilitate social distancing. Irises are unique bc of epigenetics → one person = 2 different irises. In terms of measurability, this way it is very easy to collect (no need to take off mask or wave hand) but irises are slightly harder to digitize than fingers.

[Question 5] (2 points)
Good job, you convinced the directors to use a biometric system. They have decided to acquire a fingerprint-based solution and guide users to disinfect their hands before and after presenting their fingers to the sensors. The discussion now involves (1) the need for presenting an identification card, along with the fingerprints, or (2) simply presenting the fingerprints and letting the system find who the person is. Which of these two situations is a case of **biometric verification** and which one is a case of **biometric identification**? What are the **pros** and **cons** of each approach?

1) This is biometric verification because the users are presenting their identity to the system and the system must check that the user is who they say they are based on their fingerprint similarity.
Pros: Faster to verify identity and less expensive computationally.
Cons: Since the user knows the identity of the person on the card, this system is easier to attack

2) This is biometric identification because the user is presenting only biometric data and is not claiming to be anyone. The system must then try and figure out who the person is based on its biometric database.
Pros: This system should be more secure since an attacker wouldn't know whose fingerprints to try and emulate.
Cons: This method would take longer and be more computationally costly because the system must check many database entries.

[Question 6] (2 points)
The directors have finally decided to adopt a biometric verification approach. They are planning to acquire a system that uses a single-finger USB optical sensor, whose resolution is equal to 1200 ppi, and an identification card reader. The specs say the software provides level-1, level-2, and even level-3 features. Please explain **what are these level-1, level-2, and level-3 features**. Considering the biometric verification approach, which of these feature types is the **less useful**? Please justify your answer.

Level-1 features are singular points and ridges. Level-2 features are Galton's details / minutiae like ridge bifurcations and endings. Level-3 details are things like sweat pores and scars. For verification, level-1 details are the least useful. They are often used to classify and narrow down a search, but since we are doing verification, search isn't needed. Level-2 and Level-3 are both useful. We can use level-2 for the matching, and level-3 details to prevent against common attacks.

[Question 7] (2 points)
After deciding to adopt a biometric verification approach, one of the directors was wondering if it would be possible to extend the system usage to the case of *screenings*, where a blacklist with the fingerprints of the most wanted scammers is checked every time a fingerprint is presented to the system. Regardless of the potential function creep, **are screenings closer to biometric verification or biometric identification?** Please explain your answer.

Screenings would probably be closer to biometric identification, as there would likely be a database with the data of the known scammers. The system would then need to search this database and see if there is a potential match. Because the user is not claiming an identity, this system is definitely a case of identification.

[Question 8] (2 points)
To adapt the verification system to the case of screenings, the lead software engineer of your team has come up with the following idea: wrap up the fingerprint matching routine in a loop and compare an eventually presented fingerprint with every fingerprint template belonging to the blacklist. The scammer identity should be taken as the one whose template presents the largest level-2 similarity score with the presented fingerprint. **What is the major flaw in this solution? How would you fix it?**

The major flaw in this system is that the system will always output a scammer from the blacklist. This system does not consider the fact that the person may not be on the blacklist, but instead matches it to the person their level-2 features are most similar to.

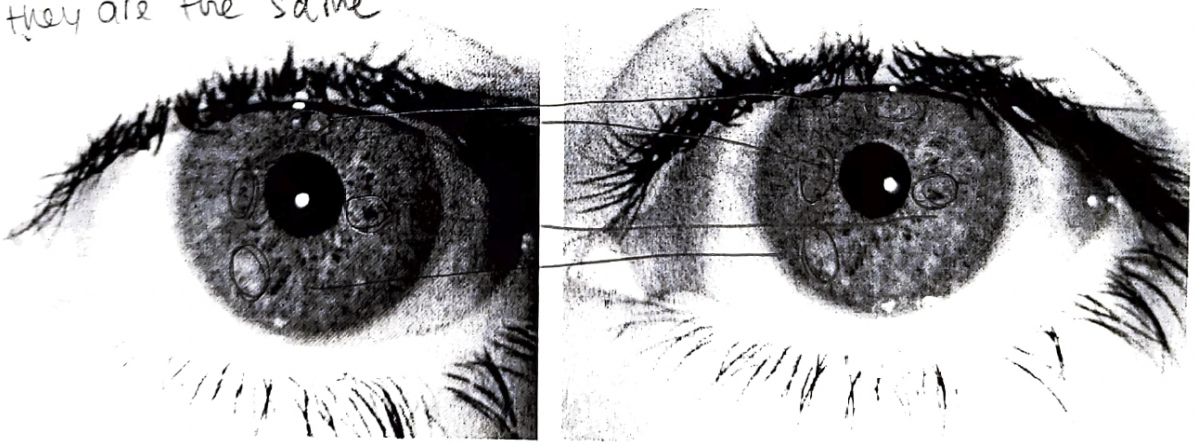
To fix this system, I would employ an open-set identification software. It would outline a certain threshold that the fingerprints must meet in order to be outputted as a match. If the threshold is not met, we can assume that the fingerprint presented is not on the blacklist.

[Question 9] (2 points)
A real case of a scientific paper submitted to a conference. While proposing a novel solution for fingerprint recognition, two authors devised an experimental setup where they have collected many fingerprint slaps from all the fingers belonging to a large set of different people. To generate genuine and impostor pairs, they decided to adopt the following approach: impostors pairs were generated by pairing individual finger slaps belonging to different people, and genuine pairs were generated by pairing individual finger slaps belonging to the same person, and to the same hand, whatever their position (pinky, ring, middle, index, and thumb). With this configuration, they provided a ROC curve of their solution over the collected dataset. **Why was their paper a straightforward reject?** Please explain your answer.

This seems ridiculous because different fingers have different prints. The "genuine" pairs would therefore also be imposters because they would not match. You would need the genuine pairs to be of the same finger.

[Question 10] (2 points)
Are the two irises below depicting the same eye? Please justify your answer by linking and naming 2-5 similar iris structures. After you've done this process manually, please **explain why it is useful and important to program computers** to do the same task.

Yes - they are the same



Getting computers to do this instead of doing it manually is important bc they can do it quicker (high throughput) they are more consistent : will always get the same results (repeatability ; predictability), and we can see why they make the decisions they do (accountability).