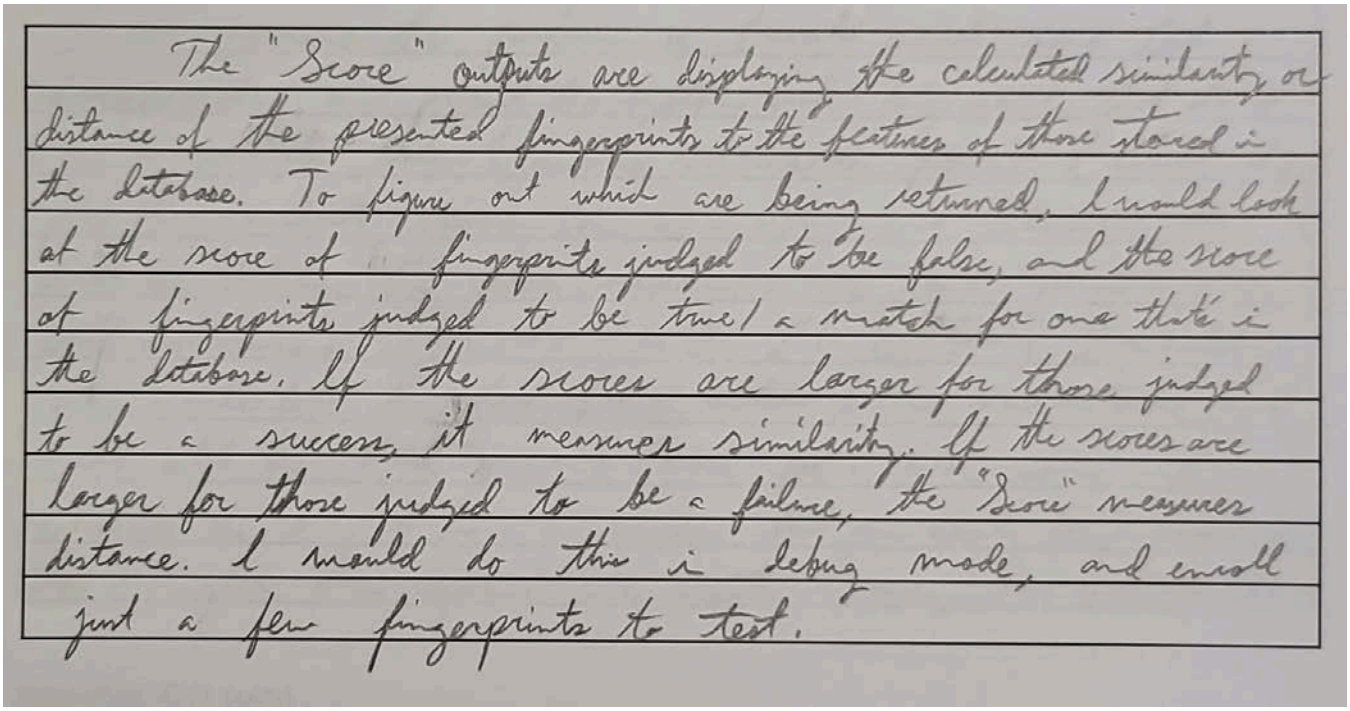
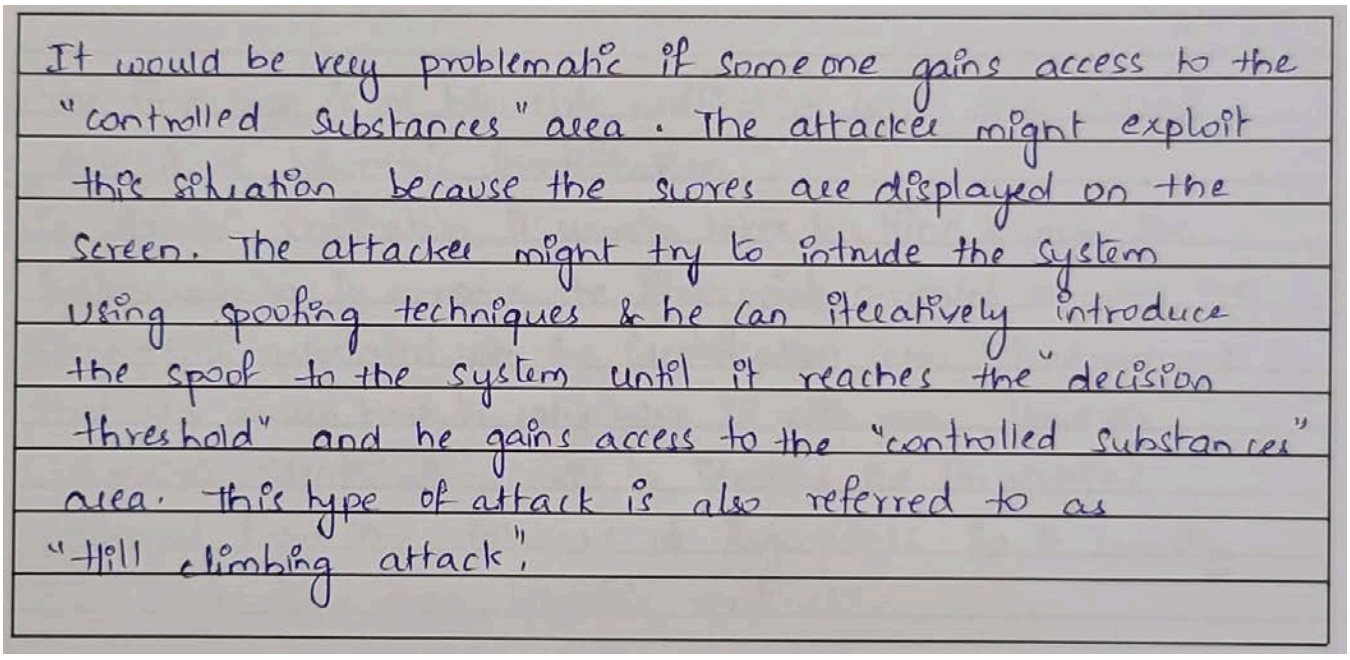
[Question 1] (1 point)
(...)

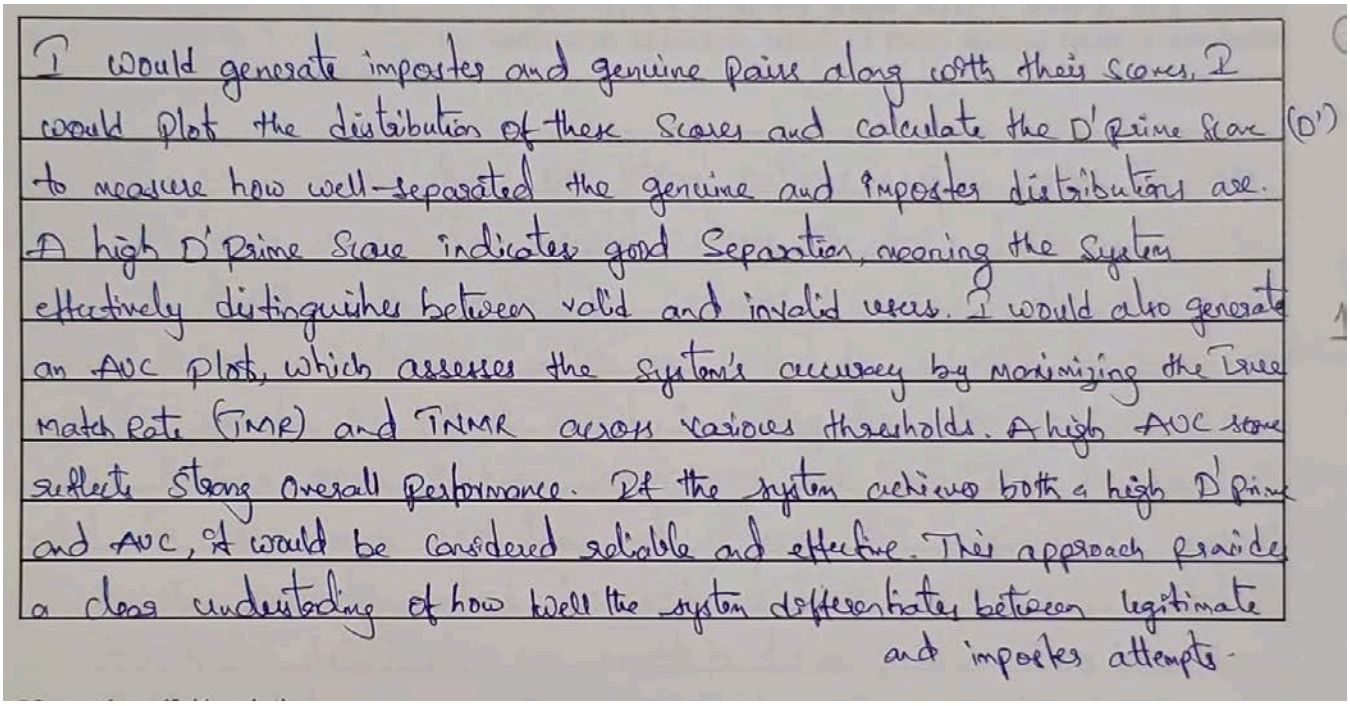
Without further information and based on your experience with biometric systems, what would the "Score" outputs in debug mode convey? How would you proceed if you were to investigate and establish their meaning (e.g., similarity or distance)? Please describe it in detail. Consider that you have the provided software fully operational; therefore, you can enroll, identify, and verify as many individuals as you want in either regular or debug modes.


The "Score" outputs are displaying the calculated similarity or distance of the presented fingerprints to the features of those stored in the database. To figure out which are being returned, I would look at the score of fingerprints judged to be false, and the score of fingerprints judged to be true/a match for one that is the database. If the scores are larger for those judged to be a success, it measures similarity. If the scores are larger for those judged to be a failure, the "Score" measures distance. I would do this in debug mode, and enroll just a few fingerprints to test.

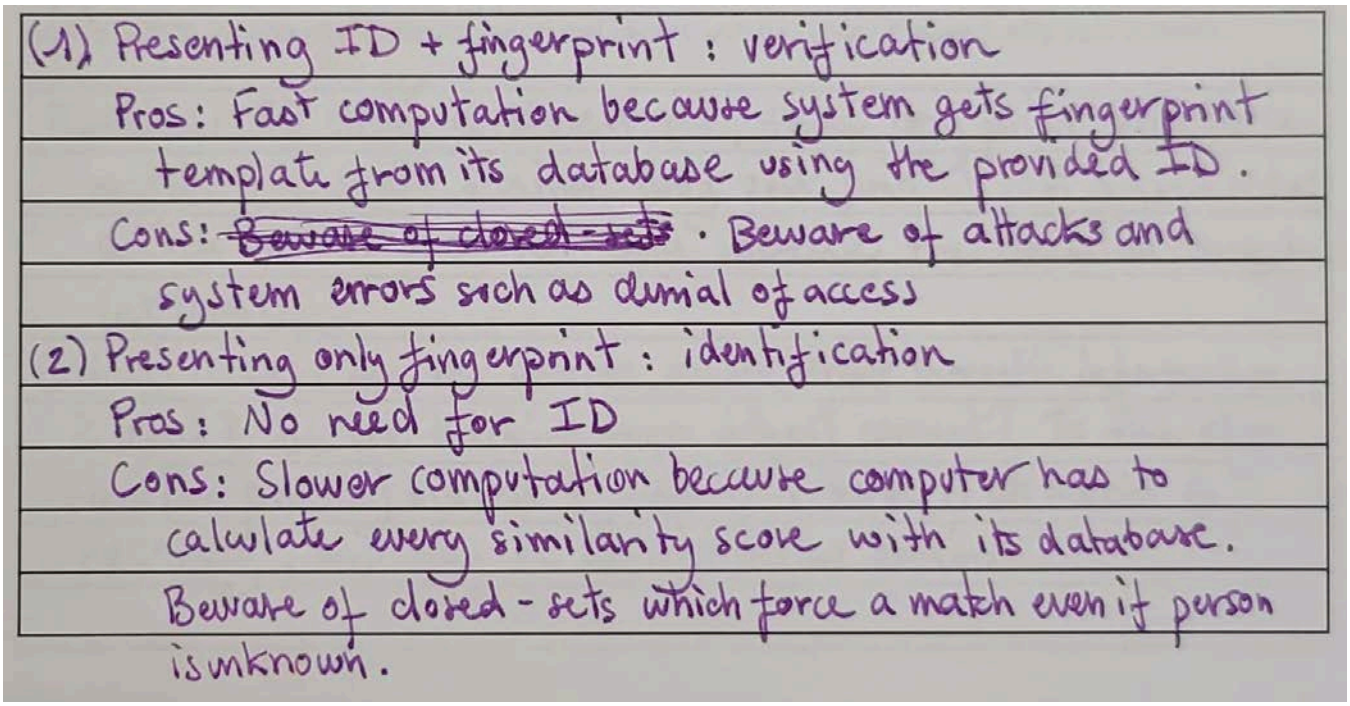
[Question 2] (1 point)
How problematic would it be to deploy this fingerprint recognition system in the production environment and let it run unwarily in debug mode? If someone were to exploit this situation, how could they attack the system? Please explain in detail.


It would be very problematic if someone gains access to the "controlled substances" area. The attacker might exploit this situation because the scores are displayed on the screen. The attacker might try to intrude the system using spoofing techniques & he can iteratively introduce the spoof to the system until it reaches the "decision threshold" and he gains access to the "controlled substances" area. this type of attack is also referred to as "Hill climbing attack".

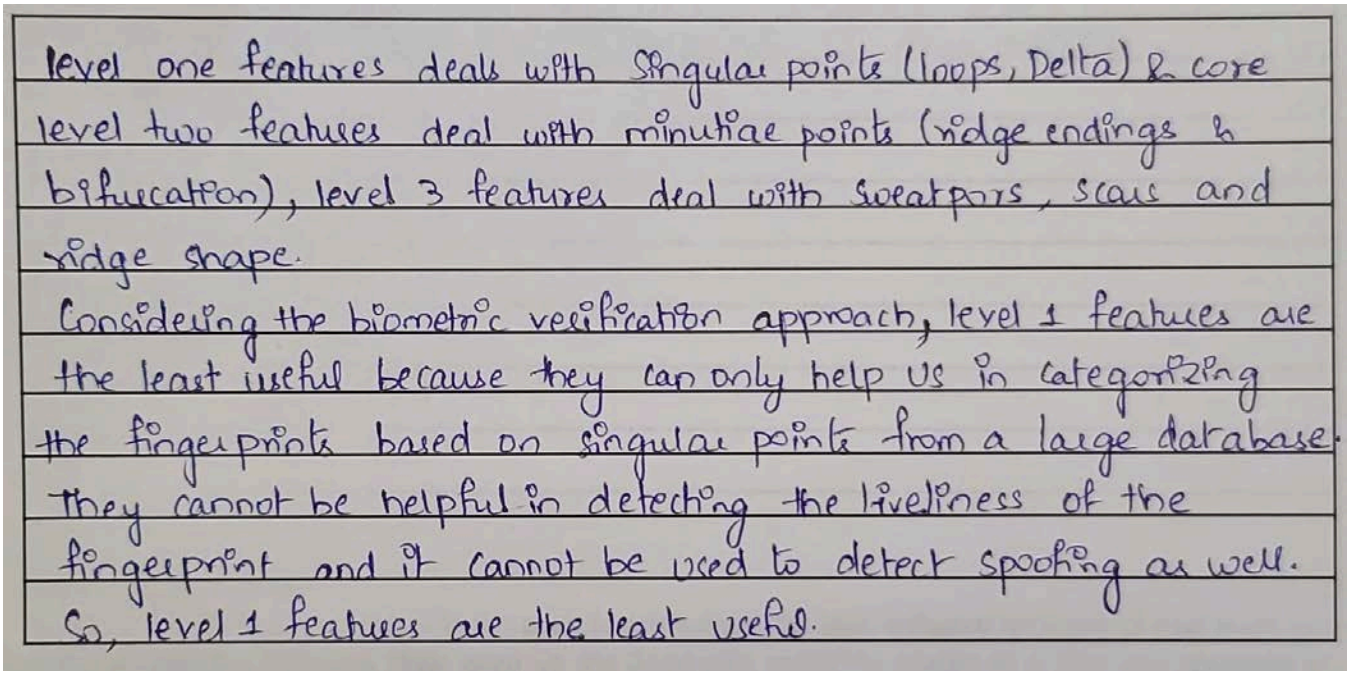
[Question 3] (1 point)
Still considering the system's "Score" outputs (either similarity or distance), if you were to measure the performance of this solution, how would you proceed? Please describe what metrics you would report and what graphs you would generate.


I would generate impostor and genuine pairs along with their scores. I would plot the distribution of these scores and calculate the D'prime score (D') to measure how well-separated the genuine and impostor distributions are. A high D'Prime Score indicates good Separation, meaning the System effectively distinguishes between valid and invalid users. I would also generate an AUC plot, which assesses the System's accuracy by maximizing the True Match Rate (TMR) and True Non-Match Rate (TNMR) across various thresholds. A high AUC score reflects Strong Overall Performance. If the system achieves both a high D'prime and AUC, it would be considered reliable and effective. This approach provides a clear understanding of how well the system differentiates between legitimate and impostor attempts.

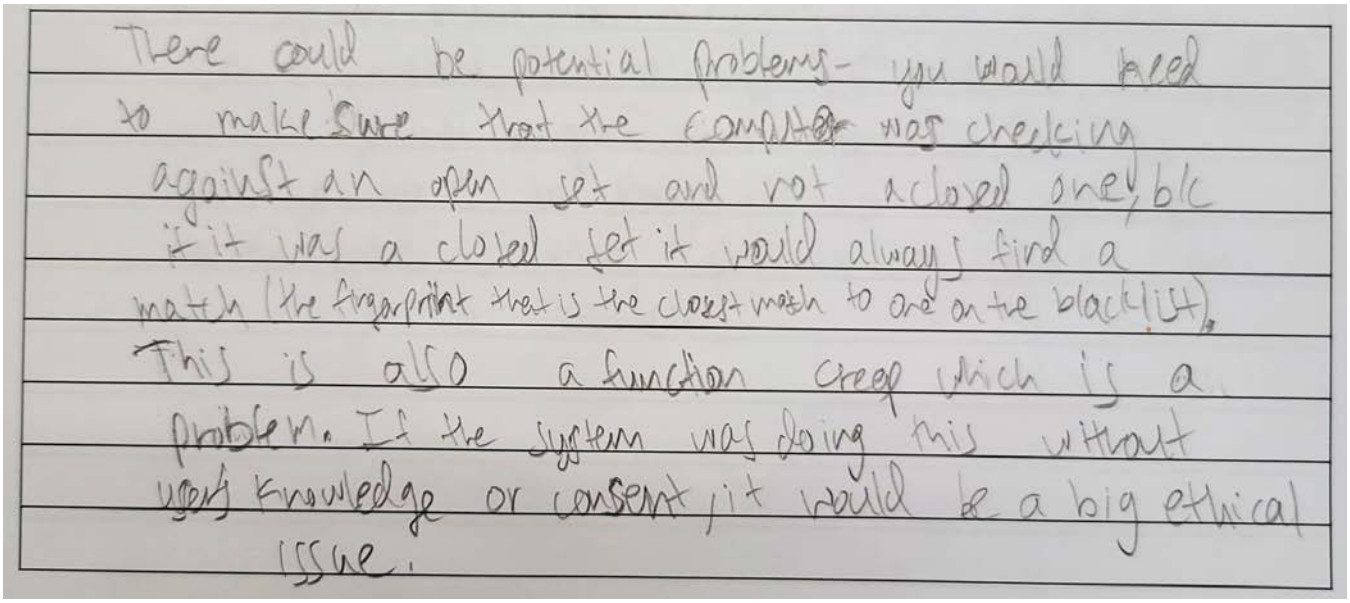
[Question 4] (1 point)
The managers of the hospital chain have decided to acquire the fingerprint recognition solution. The discussion now involves (1) the need for presenting an identification card, along with the fingerprints, or (2) simply presenting the fingerprints and letting the system find who the person is. Which of these two situations is a case of **biometric verification,** and which is a case of **biometric identification**? What are the **pros** and **cons** of each approach?


(1) Presenting ID + fingerprint : verification
Pros: Fast computation because system gets fingerprint template from its database using the provided ID.
Cons: ~~Beware of closed-sets~~. Beware of attacks and system errors such as denial of access
(2) Presenting only fingerprint : identification
Pros: No need for ID
Cons: Slower computation because computer has to calculate every similarity score with its database. Beware of closed-sets which force a match even if person is unknown.

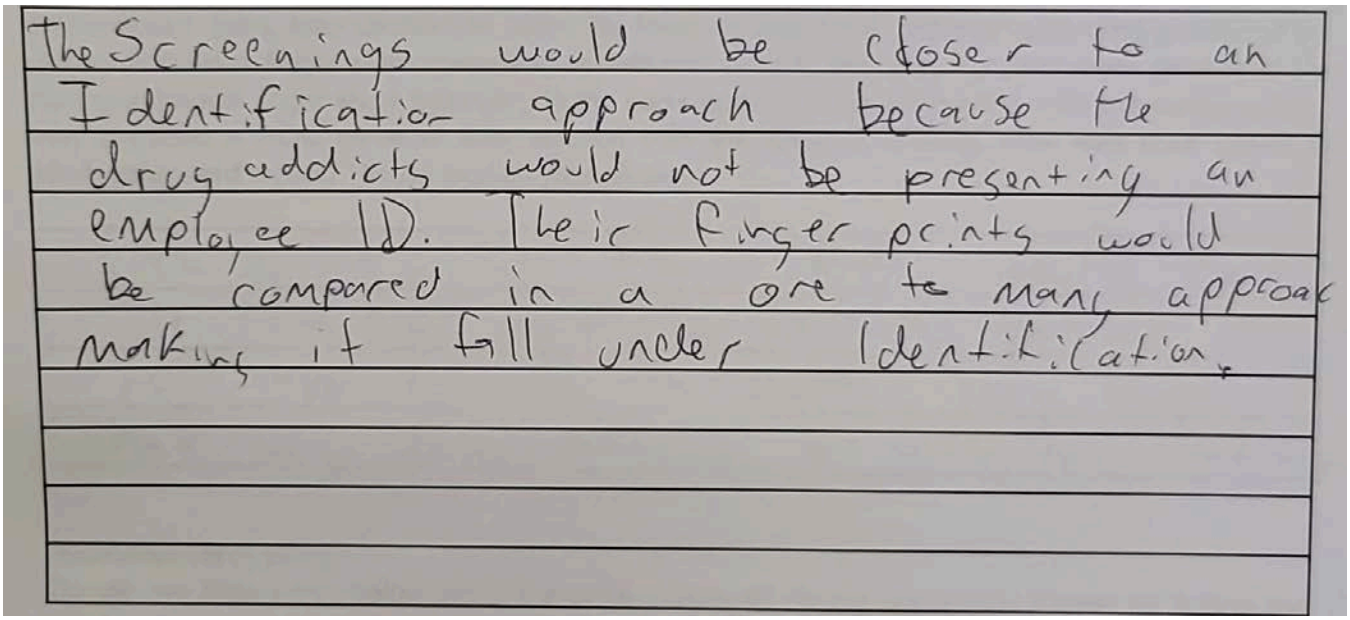
[Question 5] (1 point)
The managers have finally decided to adopt a biometric verification approach. They are planning to acquire a version of the system that uses a single-finger USB optical sensor, whose resolution is equal to 1200 ppi, and an identification card reader. The complete specs say the 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 **least useful**? Please justify your answer.


level one features deals with singular points (loops, Delta) & core
level two features deal with minutiae points (ridge endings & bifurcation), level 3 features deal with sweatpors, scars and ridge shape.
Considering the biometric verification approach, level 1 features are the least useful because they can only help us in categorizing the fingerprints based on singular points from a large database. They cannot be helpful in detecting the liveliness of the fingerprint and it cannot be used to detect spoofing as well. So, level 1 features are the least useful.

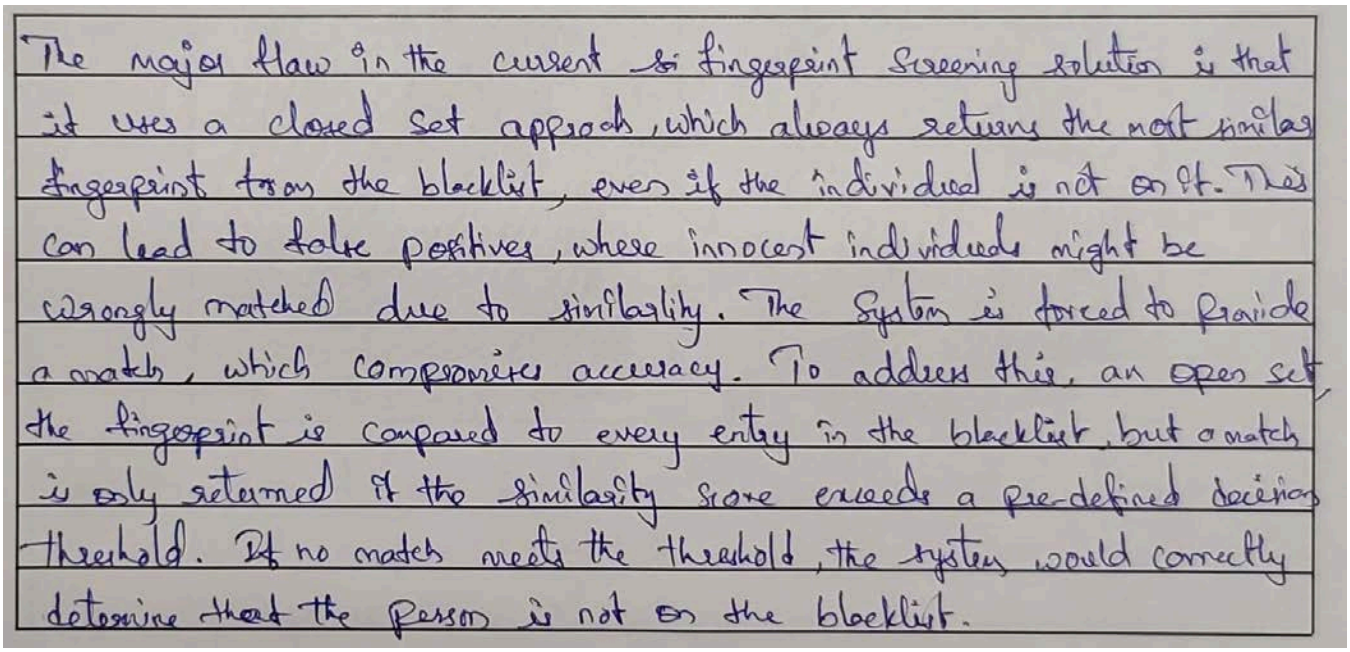
[Question 6] (1 point)
After deciding to adopt a biometric verification approach, one of the hospital directors was wondering if it would be possible to extend the system usage to the case of *screenings*, where a blocklist with the fingerprints of drug addicts would be built and then checked every time a fingerprint is presented to the system. Are there potential problems or ethical issues with this idea? Please justify your answer.


There could be potential problems- you would need to make sure that the computer was checking against an open set and not a closed one, b/c if it was a closed set it would always find a match (the fingerprint that is the closest match to one on the blacklist). This is also a function creep which is a problem. If the system was doing this without user knowledge or consent, it would be a big ethical issue.

[Question 7] (1 point)
Regardless of the problems and ethical aspects, **are screenings closer to biometric verification or biometric identification?** Please explain your answer.


The Screenings would be closer to an Identification approach because the drug addicts would not be presenting an employee ID. Their finger points would be compared in a one to many approach making it fall under Identification.

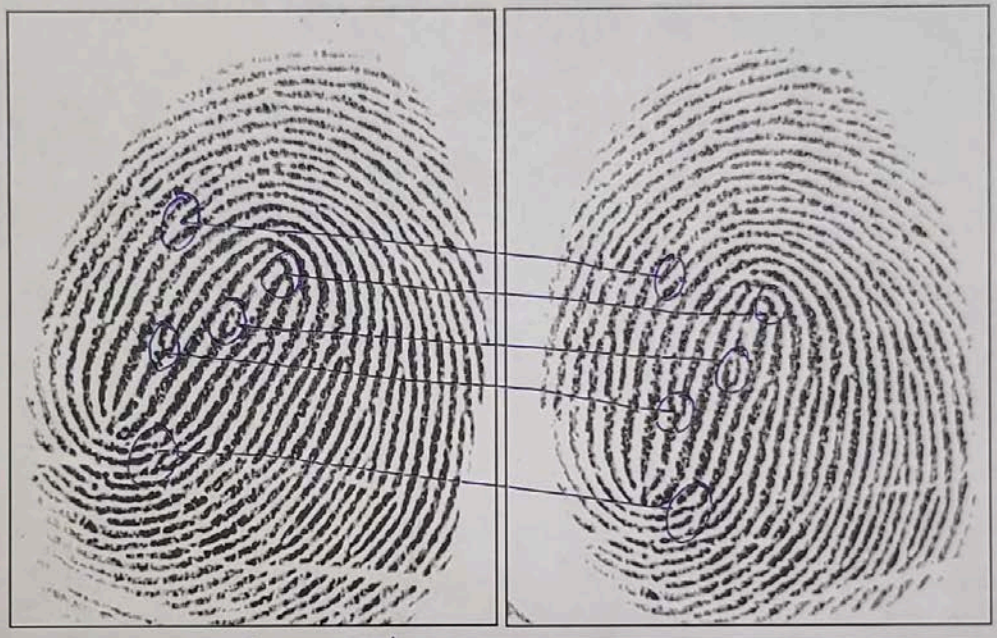
[Question 8] (1 point)
To adapt the verification system to the case of screenings, the lead software engineer of your team has come up with the following idea: wrap up the fingerprint matching routine in a loop and compare an eventually presented fingerprint with every fingerprint template belonging to the blocklist. A drug addict's identity should be taken as the one whose template presents the highest 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 the current fingerprint Screening solution is that it uses a closed set approach, which always returns the most similar fingerprint from the blacklist, even if the individual is not on it. This can lead to false positives, where innocent individuals might be wrongly matched due to similarity. The System is forced to provide a match, which compromises accuracy. To address this, an open set the fingerprint is compared to every entry in the blacklist, but a match is only returned if the similarity score exceeds a pre-defined decision threshold. If no match meets the threshold, the system would correctly determine that the person is not on the blacklist.

[Question 9] (1 point)
An actual 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 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: impostor 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, to the same hand. 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.

Did they test their system? Were they pairing the right fingers together for the genuine pairs? Different fingers would obviously have different prints, even on the same hand.

[Question 10] (1 point)
Do the two fingerprints below depict the same individual? Please justify your answer by linking and naming 5 or more similar structures within them. After you've done this process manually, please **explain why it is useful and important to program computers** to do the same task.



Yes, the two ~~individuals~~ fingerprints depict the same individual. It is useful to program computers to do this automatically because the computers are alot more quickee than humans & they tend to recognize this within seconds & with less number of errors.