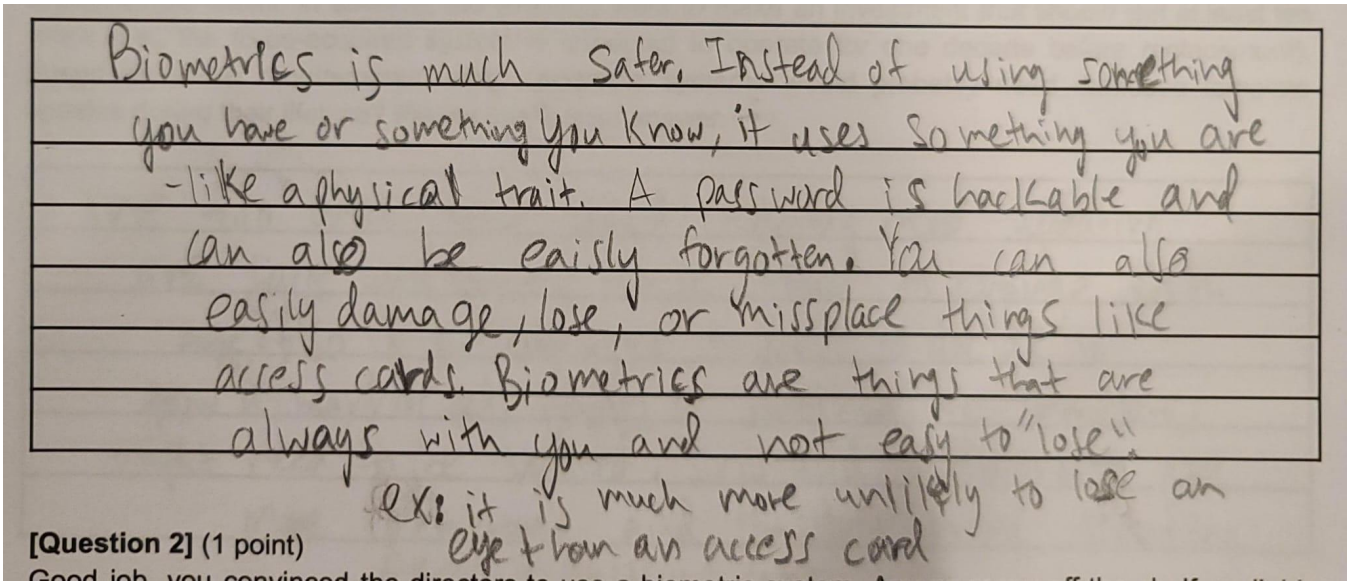
[Question 1] (1 point)
Suppose a bank company hired you to coordinate deploying an access management system to control the entrance of authorized people into the many vaults spread among their different branches. The bank directors have heard about Biometrics but are not sure about the benefits of using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


Biometrics is much safer. Instead of using something you have or something you know, it uses something you are -like a physical trait. A password is hackable and can also be easily forgotten. You can also easily damage, lose, or missplace things like access cards. Biometrics are things that are always with you and not easy to "lose". ex: it is much more unlikely to lose an eye than an access card

[Question 2] (1 point)
Good job, you convinced the directors to use a biometric system. Among many off-the-shelf available solutions, four well-documented systems caught your attention. The table below summarizes these solutions after a careful reading of their specs.

	System 1	System 2	System 3	System 4
Trait	Voice	Face	Fingerprint	Iris
AUC	0.96	0.98	0.97	0.92
d-prime	2.94	4.09	2.80	2.35
FMR @ EER	0.0675	0.0027	0.0554	0.0912
FNMR @ EER	0.0675	0.0027	0.0554	0.0912
Price	$25,000.00	$10,000.00	$2,500.00	$5,000.00
Runtime (comparisons per sec.)	2,500	1,000	1	100
Database storage (MB per 100k individuals)	160	200	2	780

If you were to choose one system based solely on accuracy and ignoring the other aspects (such as trait, price, runtime, memory footprint, number of employees, and system lifetime), what solution would you select? Please justify your answer.

I would choose system 2 because it has the highest AUC and d-prime, as well as the lowest FMR and FNMR at EER.

[Question 3] (1 point)
Your company just brought some more information to the table. Only around 50 employees will need access to the vaults. In addition, the directors want to make an investment that should last at least ten years (i.e., the to-be-acquired system is expected to operate for one decade before replacement). Based on these requirements, what candidate systems would probably need database template updates during their lifetime? Please justify your answer.

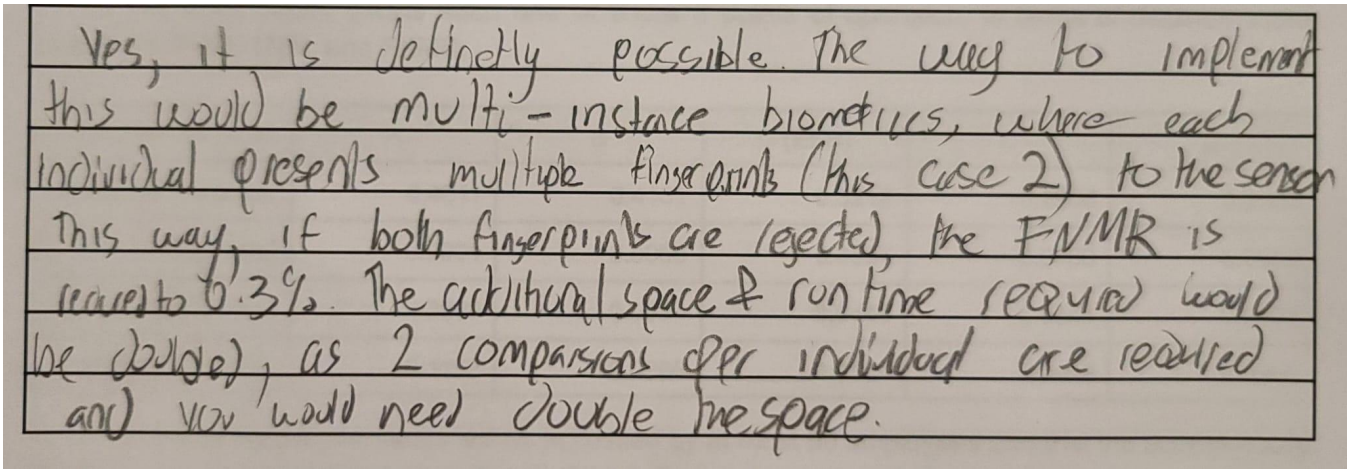
Systems 1 and 2 would most likely require database template updates during their lifetime because the traits they measure, voice and face, change over time as an individual ages. Someone may look and sound different than they did 10 years ago.

[Question 4] (1 point)
One director was intrigued that the two cheapest systems altogether cost less than the other solutions. She was wondering if there is any advantage to acquiring these two systems instead of a single and more expensive one. Does she have a good point? What would be the possibilities if the company acquires the two cheapest solutions? Would you be able to leverage them both? If you would, please explain how you could do it.

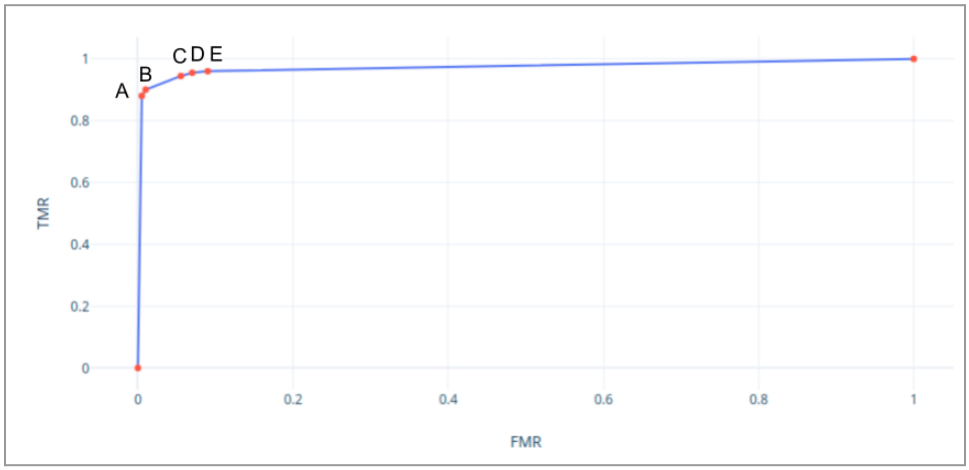
Yes you could use both of them. This would be a multi-modal multibiometric system. You could run these systems in either cascade or parallel fashion, making results more accurate. You can also use score level fusion and establish thresholds and decide whether or not to grant access with AND and OR operations

[Question 5] (1 point)
One of the software engineers of the company came to you claiming that he knows how to leverage the cheapest fingerprint-based solution alone in a way that improves its FNMR from 0.0554 (5.54% probability of false rejection) to 0.0554 x 0.0554 = 0.00306916 (0.306916% probability of false rejection), with nearly no additional operational cost (no need for extra sensors or extra software modules but only an affordable increase in runtime and template database storage). He says that with his idea, the runtime goes from 1 comparison per second to 1 authentication every two seconds, and the database storage increases from 2 MB per 100k enrolled individuals to 4 MB per 100k individuals. Do you think this is possible? If you do, please explain how it can be done. If you don't, please explain why and regarding which assumptions he might be wrong.

Useful tip. Imagine you're in a game with dice and lose whenever you get all the dice facing the one-dot side after tossing them. With one dice, your probability of losing is 1/6. With two dice, you lose only when you get one dice facing one dot AND the other dice also facing one dot; hence, the probability of losing is 1/6 x 1/6 = 1/36. Analogously, in a biometric system, you lose whenever you get only false rejections.


Yes, it is definetly possible. The way to implement this would be multi-instance biometrics, where each individual presents multiple fingerprints (this case 2) to the sensor. This way, if both fingerprints are rejected the FNMR is reduced to 0.3%. The additional space & runtime required would be doubled, as 2 comparisons per individual are required and you would need double the space.

[Question 6] (1 point)
The following graph depicts the ROC curve of the cheapest solution (fingerprint-based), whose AUC is 0.97. This graph highlights five interesting operation points, from A to E. Point C corresponds to the system operation at an equal error rate (EER), when FNMR = FMR = 0.0554, and the decision score threshold is set to 0.3212. In this configuration, the system wrongly rejects nearly 5% of genuine authentications (i.e., one in every twenty genuine users is wrongly denied access, hence FNMR=0.0554), and it wrongly accepts 5% of impostor authentications (i.e., one in every twenty impostor users is wrongly granted access, hence FMR=0.0554). This FMR, in particular, is unacceptable for ensuring the security of the company's vaults.



The table below details each one of these 5 points of operation, in terms of decision score **threshold**, **FMR**, **TMR**, and **FNMR**.

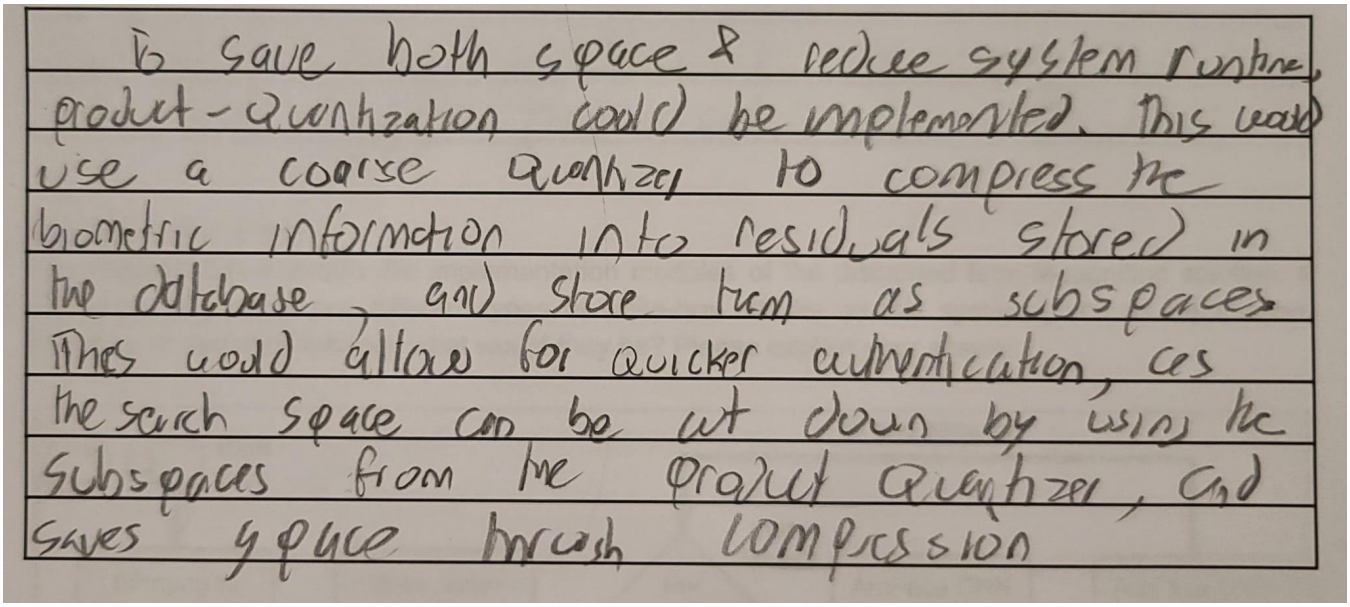
Point of Operation	A	B	**C (EER)**	D	E
Decision Threshold	0.4511	0.4131	**0.3212**	0.2956	0.2585
FMR (x axis)	0.0001	0.0050	**0.0554**	0.0700	0.0900
TMR (y axis)	0.8802	0.9004	**0.9446**	0.9551	0.9601
FNMR (1.0 - TMR)	0.1198	0.0996	**0.0554**	0.0449	0.0399

Considering that the vaults will be accessed by at most 50 employees and that the access doors always count on an assisted surveillance desk with security guards in front of it, the FMR and FNMR values can be tweaked (i.e., either relaxed or reinforced) according to this scenario. For example, with only 50 folks to authenticate daily, it might not be a big deal to wrongly deny access to five of them every day (i.e., tolerate a FNMR of 10%), considering that the guards will be there to supervise these situations and manually let the five wrongly denied folks in. In this case, a low FMR is much more important than a low FNMR, indicating that the operation at EER might not be the best choice.

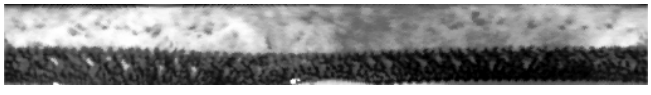
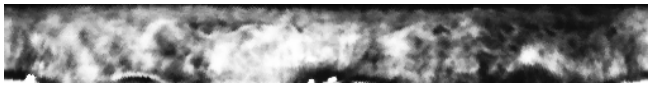
Given these considerations, is there a way to still use the cheapest fingerprint-based biometric system with no fusion at all? If you were to do it, how would you proceed? Please justify your answer.

Yes, I believe it would be possible to still use this fingerprint-based system by setting the threshold to 0.4511 to ensure the security of the system so that the FMR is 0.01% and prevents impostors from accessing the system in most cases. In this case, the FNMR would be 11.98%, meaning the guards would have to manually let in the 5 or 6 people who were denied access. I also think it would be acceptable to use B as the threshold so that the FNMR is a little lower but the system is still very secure.

[Question 7] (1 point)
After some debate and due to better lifetime support offered by the respective manufacturer, your company decided to acquire the iris recognition system to authenticate both eyes of the employees. This system thus spends 2 x 780 = 1560 MB of disk for every 100k enrolled individuals (given both eyes are enrolled). If you were to use this system in a large-scale scenario for authenticating millions of individuals, what feature indexing strategies would you use to (1) speed up the authentication process and reduce the system runtime, and (2) reduce the disk space spent to store the enrolled iris templates. Please justify your choices of feature indexing method.



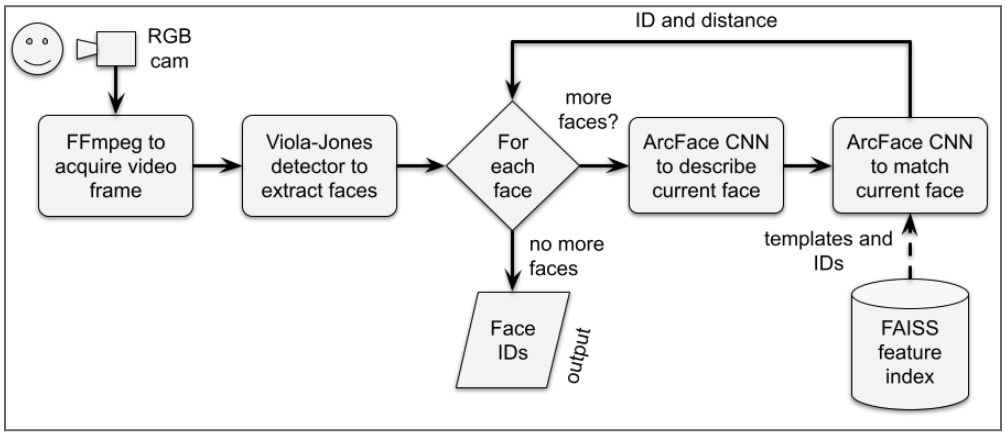
[Question 8] (1 point)
Congratulations! After your guidance, the iris recognition system was acquired, set up, and deployed in your company. The solution seems to be working satisfactorily, except for an awkward situation. On the occasion of adding a particular new employee, the system operator noticed a failure-to-enroll (FTE) error while trying to add her second iris. After going through the system logs, the operator noticed a conflict between her first and second irises, as if they were the same. The operator made sure he was not enrolling the same eye twice by mistake. The figures below depict the two acquired irises (left-side column) after proper normalization, and put them in perspective with random regular working irises, which were successfully enrolled into the system (right-side column).

Employee's conflicting irises	Regular working irises
	
	

Based on your experience, is it possible for someone to have left and right irises nearly the same? Please justify your answer. In the case you claim it is not possible, what could be the reason for the FTE error, based on the images above?

No, it is impossible to have the same or nearly identical irises. Irises are epigenetic so each one is unique. The reason for this error may be because the person is wearing contact lenses with a pattern printed on them, such as a contact lense with a different colored eye. This printed pattern would be identical, and would obfuscate the real eye, confusing the sensor

[Question 9] (1 point)
The diagram below details the implementation modules of the discarded face recognition solution. If you were to perform two different types of white-box attacks on this system (such as repudiation, spoofing, or denial of service), what would they be? Please explain your answer.



I could utilize make-up to conduct a spoofing attacks on the system, by altering my face in a way that matches someone's identity. Repudiation could also make by obscuring my face with makeup such that it isn't recognizable Denial of service would be another attack, by wearing a shirt with a specific pattern to flood the Viola-Jones detector, by "generating" unlimited faces to present to the system

[Question 10] (1 point)
Are the two irises below depicting the same eye? Please justify your answer by linking and naming 2-5 similar iris structures.