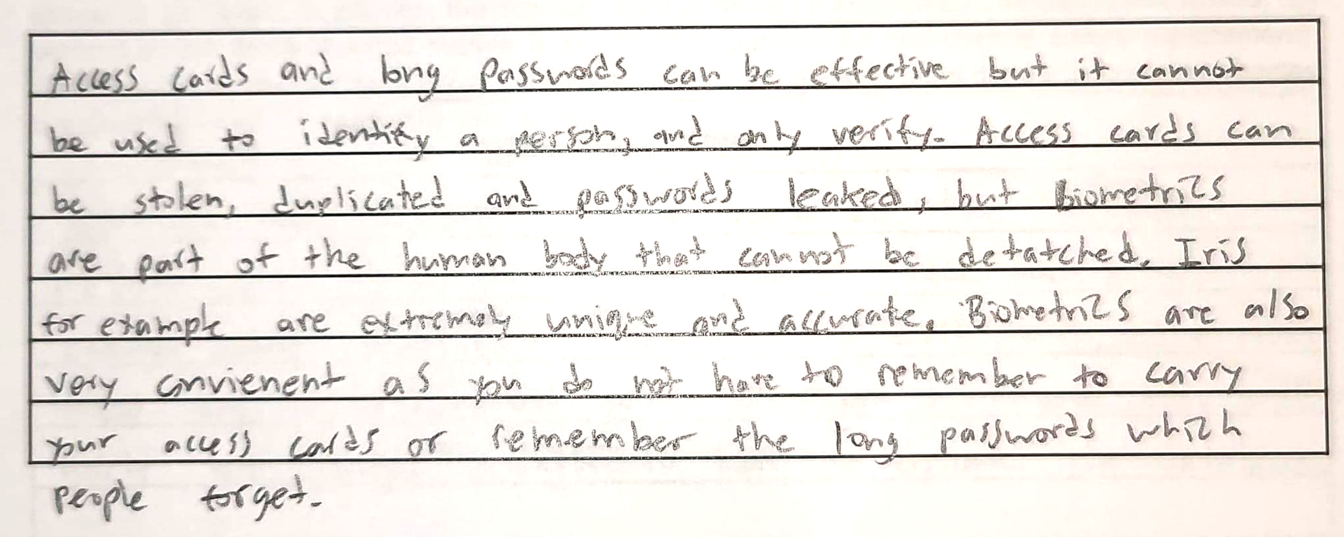
[Question 1] (1 point)
Suppose a bank company hired you to coordinate deploying an access management system to control the entrance of authorized people into the many vaults spread among their different branches. The bank directors are aware of Biometrics but question its benefits. They think using access cards and long passwords is as effective and cheaper than acquiring and hosting a biometric system. **What would you say to convince them** if it is your duty to change their mind?



Access cards and long passwords can be effective but it cannot be used to identify a person, and only verify. Access cards can be stolen, duplicated and passwords leaked, but biometrics are part of the human body that cannot be detatched. Iris for example are extremely unique and accurate, Biometrics are also very convienent as you do not have to remember to carry your access cards or remember the long passwords which people forget.

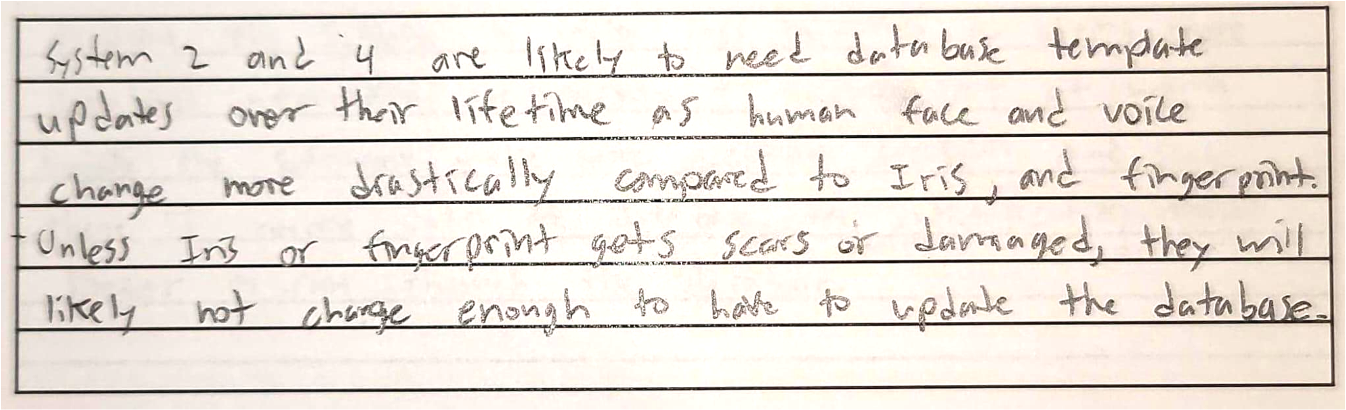
[Question 2] (1 point)
Good job, you convinced the directors to use a biometric system. Among the many off-the-shelf solutions available, four well-documented systems caught your attention. The table below summarizes these solutions after a careful reading of their specs.

	System 1	System 2	System 3	System 4
Trait	Fingerprint	Face	Iris	Voice
AUC	0.96	0.98	0.92	0.95
d-prime	2.80	4.09	2.35	2.94
FMR @ EER	0.0554	0.0027	0.0912	0.0675
FNMR @ EER	0.0554	0.0027	0.0912	0.0675
Price	$2,500.00	$10,000.00	$5,000.00	$25,000.00
Runtime (authentications per sec.)	1	1,000	100	2,500
Database storage (MB per 100k individuals)	2	200	780	160

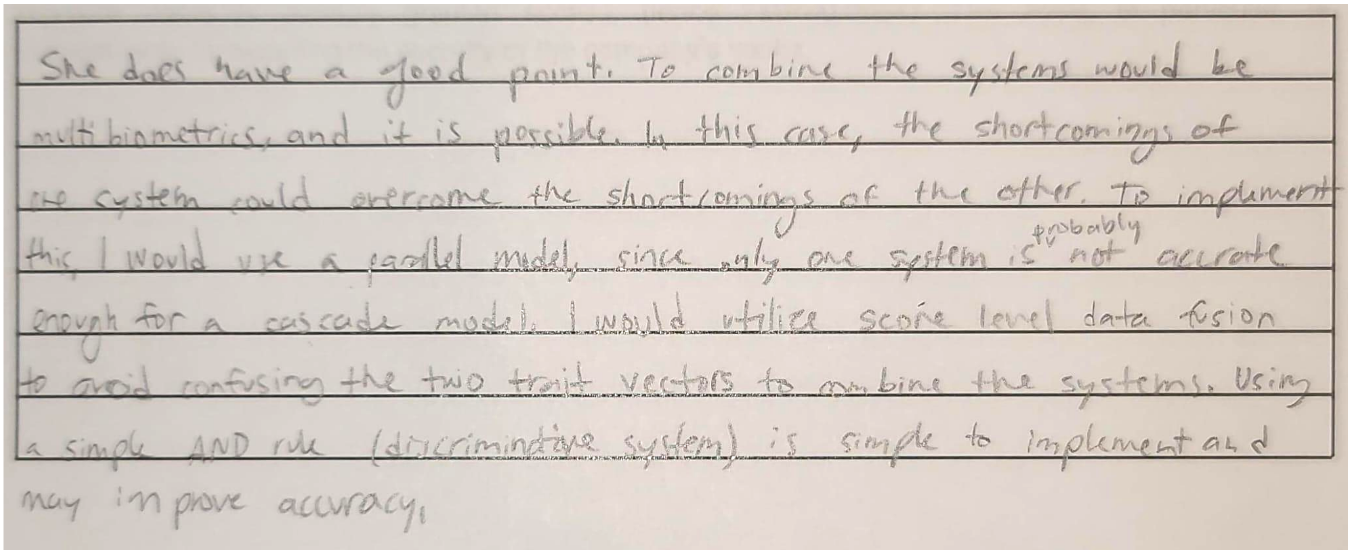
If you were to choose one system based solely on **accuracy** and ignoring the other aspects (such as trait, price, runtime, memory footprint, and system lifetime), what solution would you select? Please justify your answer.

Face. It has both the highest AUC and d-prime values. It also has the lowest FMR and FNMR @ 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, which candidate systems are likely to need database template updates over their lifetimes? Please justify your answer.


System 2 and 4 are likely to need database template updates over their lifetime as human face and voice change more drastically compared to Iris, and fingerprint. Unless Iris or fingerprint gets scars or damaged, they will likely not change enough to have to update the database.

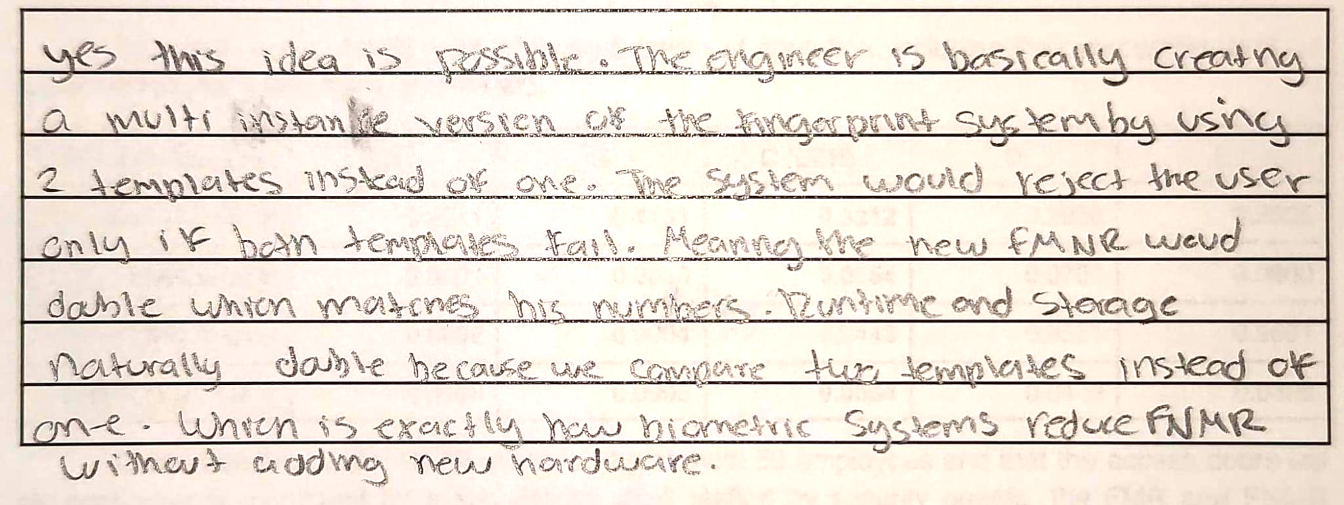
[Question 4] (1 point)
One director was intrigued that the two cheapest systems altogether cost less than the other solutions. She was wondering whether there is any advantage to acquiring these two systems instead of a single, more expensive one. Does she have a good point? What would the possibilities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


She does have a good point. To combine the systems would be multibiometrics, and it is possible. In this case, the shortcomings of one system could overcome the shortcomings of the other. To implement this I would use a parallel model, since only one system is probably not accurate enough for a cascade model. I would utilize score level data fusion to avoid confusing the two trait vectors to combine the systems. Using a simple AND rule (discriminative system) is simple to implement and may improve accuracy.

[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 0.0554^2 = 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 increases from 1 authentication 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 to do it. If you don't, please explain why and which assumptions he might be wrong about.

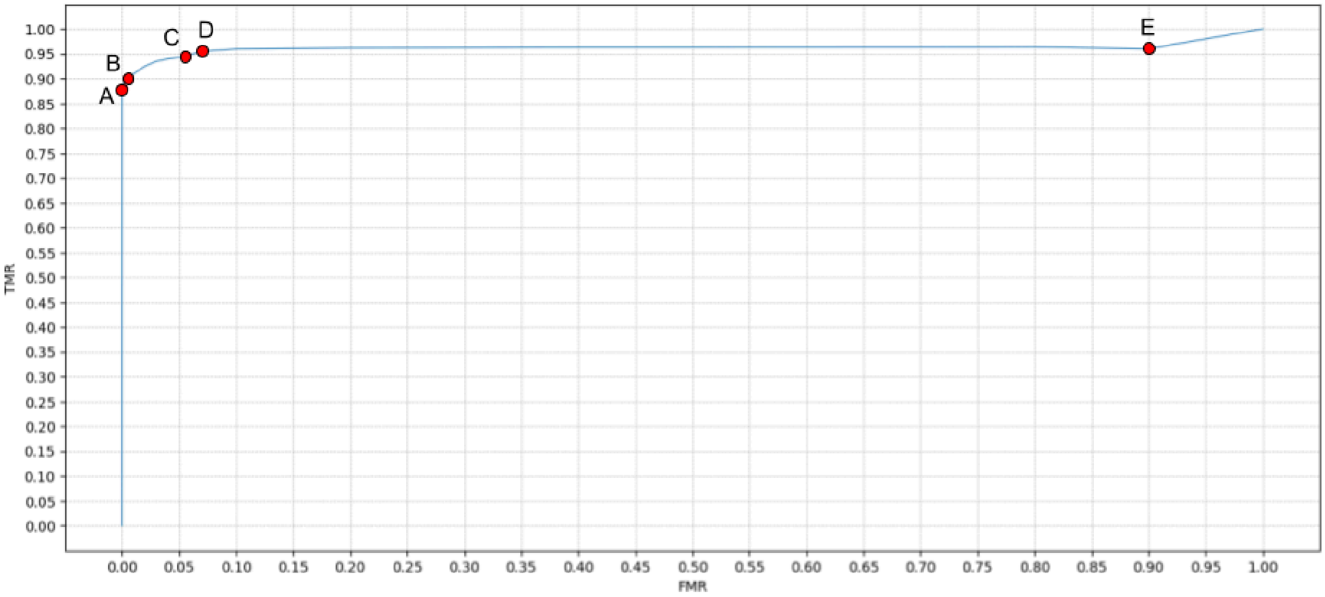
Useful tip. Imagine you're in a game with dice and lose whenever you get all the dice facing the one-dot side after tossing them. With one dice, your probability of losing is 1/6. With two dice, you lose only when you get one dice facing one dot AND the other dice also facing one dot; hence, the probability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



yes this idea is possible. The engineer is basically creatng a multi instance versien of the fingerprint system by using 2 templates instead of one. The system would reject the user only if both templates fail. Meaning the new FMNR woud dauble which matches his numbers. Runtime and storage naturally dauble because we compare two templates instead of one. Which is exactly how biometric systems reduce FNMR without adding new hardware.

[Question 6] (1 point)

The following graph depicts the ROC curve for the cheapest solution (fingerprint-based), with an AUC of 0.9621. This graph highlights five interesting points of operation, from A to E. Point C corresponds to the system operating at equal error rate (EER), with FNMR = FMR = 0.0554 and a decision score threshold of 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.

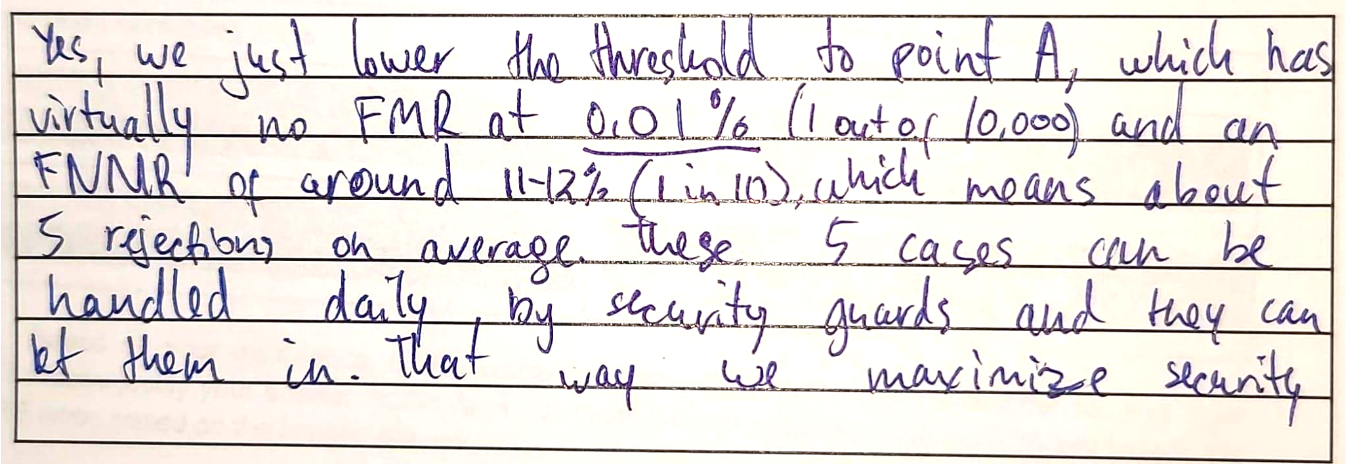


The table below details each of these 5 points of operation, including their respective decision score **threshold**, **FMR**, **TMR**, and **FNMR**.

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

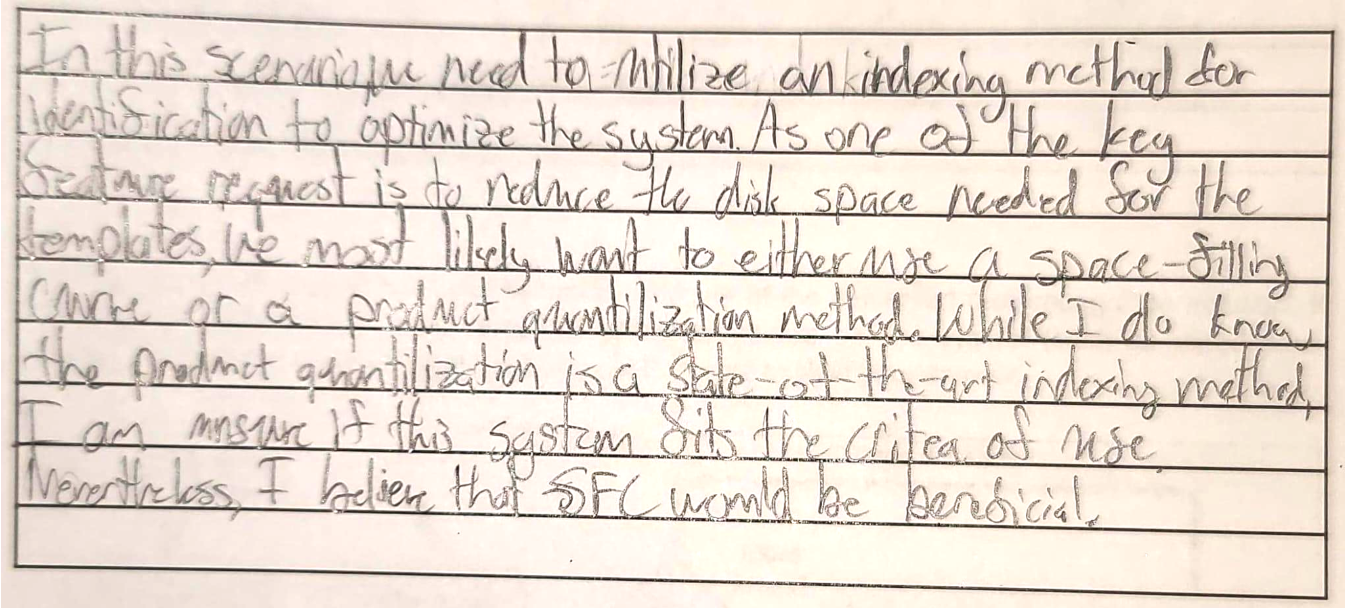
Given that the vaults will be accessed by at most 50 employees and that the access doors will be continuously monitored by a surveillance desk staffed by security guards, the FMR and FNMR values can be adjusted (i.e., relaxed or reinforced) accordingly. For example, with only 50 folks to authenticate 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, suggesting that operating at EER might not be the best choice.

Given these considerations, is there a way to still use the cheapest fingerprint-based biometric system without any fusion? If you were to do it, how would you proceed? Please justify your answer.



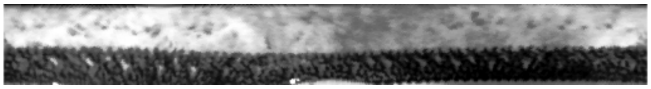
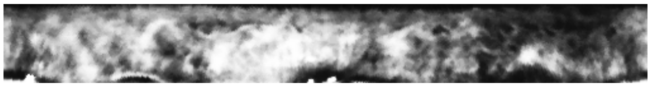
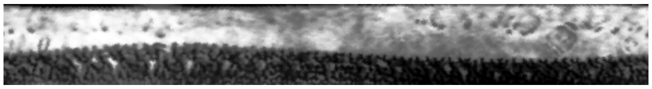
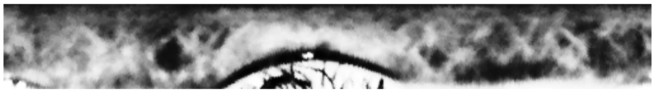
Yes, we just lower the threshold to point A, which has virtually no FMR at 0.01% (1 out of 10,000) and an FNMR of around 11-12% (1 in 10), which means about 5 rejections on average. these 5 cases can be handled daily by security guards and they can let them in. That way we maximize security

[Question 7] (1 point)
After some debate and after considering the better lifetime support offered by the manufacturer, your company decided to acquire the iris recognition system to authenticate both employees' eyes. This system thus consumes 2 × 780 = 1560 MB of disk space for every 100k enrolled individuals (assuming 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.



In this scenariowe need to utilize an indexing method for identification to optimize the system. As one of the key feature request is to reduce the disk space needed for the templates, we most likely want to either use a space-filling curve or a product quantilization method. While I do know, the product quantilization is a state-of-the-art indexing method, I am unsure if this system fits the critea of use. Nevertheless, I believe that SFC would be beneficial.

[Question 8] (1 point)
Congratulations! After your guidance, the iris recognition system was acquired, set up, and deployed in your company. The solution is working satisfactorily, except for an awkward situation. During the enrollment of a new employee, the system operator encountered a failure-to-enroll (FTE) error while attempting 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 irises, which were successfully enrolled into the system (right-side column).

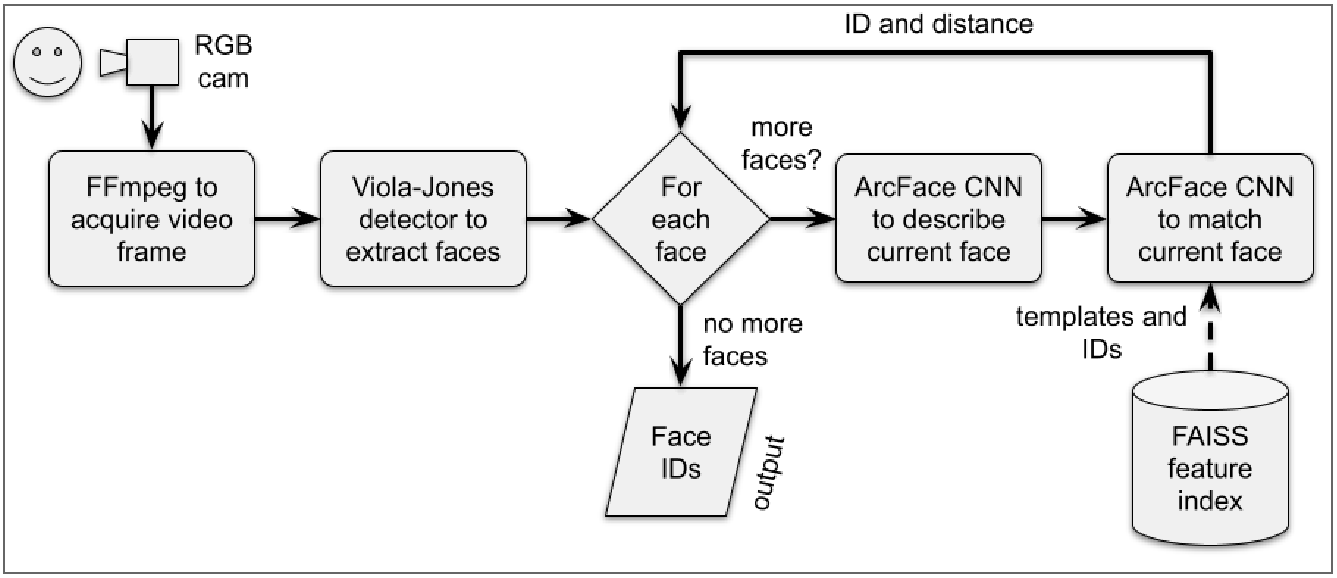
Employee's conflicting irises	Random regular irises
	
	

Based on your experience, is it possible for someone to have nearly identical left and right irises? 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?

Irises are epigenetic meaning no It isn't possible for someone to have Identical right and left irises. likely they are using colored contact lenses that change the appearence of their eyes. These lenses are not unique and thus is why they appear the Same.

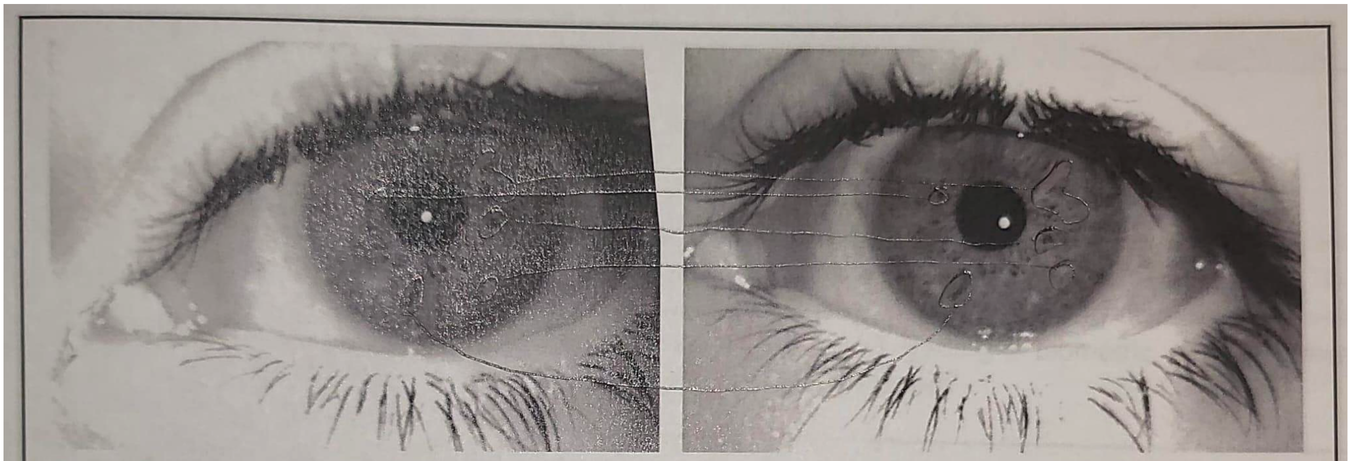
[Question 9] (1 point)

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.


RGB cam
FFmpeg to acquire video frame
Viola-Jones detector to extract faces
For each face
more faces?
ArcFace CNN to describe current face
ArcFace CNN to match current face
ID and distance
no more faces
Face IDs
output
templates and IDs
FAISS feature index

Since it is only grabbing a Single frame, I could likely Spoof the System with a presentation attack by Showing a photo of a face thats in the system. Since Viola-jones uses Haar-like features to detect faces I could paint my face to confuse the system; allowing repudiation.

[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.



Yes, these irises are the same eye. There is a crypt in the bottom
left that appears in both eyes as well as a lighter spot in the
top right of the eye. Additionally, the crypts surrounding the pupil
match in shape and location.