Homework 1

CSE 402 - Biometrics and Pattern Recognition

Instructor: Dr. Arun Ross

Due Date: September 21, 2022 (11:00 pm)

Total Points: 60

Note:

Q **You are permitted to discuss the following questions with others in the class.**

Q **However, you *must* write up your *own* answers to these questions. Any indication to the contrary will be considered an act of academic dishonesty.**

Q **A neatly typed report with detailed answers is expected. The report must be uploaded in D2L in PDF format.**

Q **All outputs, such as graphs and images, must be included in the report.**

Q **Any code developed as part of the assignment must be (a) included as an appendix in the report, as well as (b) archived in a single zip file and uploaded in D2L.**

Q **Include a bibliography at the end of the report indicating the resources that you used (e.g., URL, scientific articles, books, etc.) to complete this homework.**

Q **Please submit the report (PDF) and the code (Zip file) as two separate files in D2L.**

---

1. [15 points] Read the following paper by Patel et al. and answer the questions below. You answer must be written clearly and in complete sentences.

   PATEL et AL., "Continuous User AUTHENTICATION on Mobile Devices: Recent Progress AND REMAINING CHAL- lenges," in IEEE SIGNAL Processing MAGAZINE, vol. 33, no. 4, pp. 49-61, July 2016. [PDF]

   (a) What is *continuous AUTHENTICATION*? Why is it necessary?

   Ans) Continuous authentication is nothing but the constant monitoring on your mobile device even after granting the initial access. Continuous authentication was created as many users of mobile devices found loopholes in the traditional methods for authentication. So, biometrics and security research communities came together and developed the continuous authentication this authentication makes use of physiological and behavioral biometrics of the user. These biometrics are gathered and are used to monitor identity by using built in sensors and accessories such as the gyroscope, touch screen, accelerometer, orientation sensor, and pressure sensor.

   With the advancements in technology mobile devices can store a lot of data to protect the mobile devices from data leaks the continuous authentication adds an extra layer of security to the mobile devices so that unauthorized users are restricted from accessing the data in the device.

(b) What are some of the other terms used in the literature in order to refer to continuous authentication?

Ans) Some of the other terms used in the literature in order to refer to continuous authentication are:

- Active authentication
- Implicit authentication
- Transparent authentication

(c) What are some of the limitations of *explicit* authentication mechanisms such as passwords and PINs?

Ans) The limitations of using explicit authentication mechanism are:

- When a person is trying to set up a pin or password for his phone most of them use common pin numbers that are very easy for the hackers to guess it. This way your phone becomes less secure and could be easily accessed by the hackers which can be a danger.

- When it comes to pattern type of lock people keep on using the same pattern again and again which leaves your finger marks on the screen which resemble the exact pattern that you use to unlock your phone making it easy for the hacker to analyze it and guess the pattern using some special tools.

(d) Describesomeofthebiometricattributesthatcanbeusedforcontinuousauthentication.

Ans) Continuous authentication uses physiological and behavioral biometric attributes such as face recognition, which is done by the front camera, touch gestures, hand movements & fingerprint scanner these three attributes are analyzed by the gyroscope, touch screen and accelerometer.

(e)What are some of the *USABILITY* and *security* issues related to the deployment of continuous authentication mechanisms on mobile devices?

Ans) There are drawbacks to every security system. People will tolerate false rejection than false acceptance like if your trying to unlock your mobile with a face id and it rejects you to be a legitimate user because your face wasn't in a right position or your eyes were closed whatever reason it could be but, if the same mobile phone accepts someone's else's face and gives him the access then you are concerned about the security of the device. These false acceptance, delays and false rejects are the main usability and security concerns while deploying continuous authentication mechanism on mobile devices.

2. [10 points] Consider an experiment in which you are provided the face images of 10 subjects. The number of images collected from each subject is tabulated below:

Subject Number	Number of Images
001	4
002	8
003	1
004	2
005	9
006	7
007	11
008	6
009	5
010	3

Based on these numbers, what is the number of genuine scores and the number of impostor scores that can be generated using a symmetric face matcher? Explain your answer.

Ans) Genuine Scores: N *(mC2)

= (4!/2!*2!) + (8!/2!+6!) + (2!/2!*0!) + (9!/2!*7!) + (7!/2!*5!) + (11!/2!*9!) + (6!/2!*4!) + (5!/2!*3!) + (3!/2!*1!)

= 6 + 28 + 1 + 36 + 21 + 55 + 15 + 10 + 3

= 175

Total number of images: 56

Total Scores: (N*mC2)

= (56!) / 2!*(54!)

= 1540

Impostor Scores = Total Scores – Genuine scores = 1540 – 175 = 1365

Genuine Scores: 175

Impostor Scores: 1365

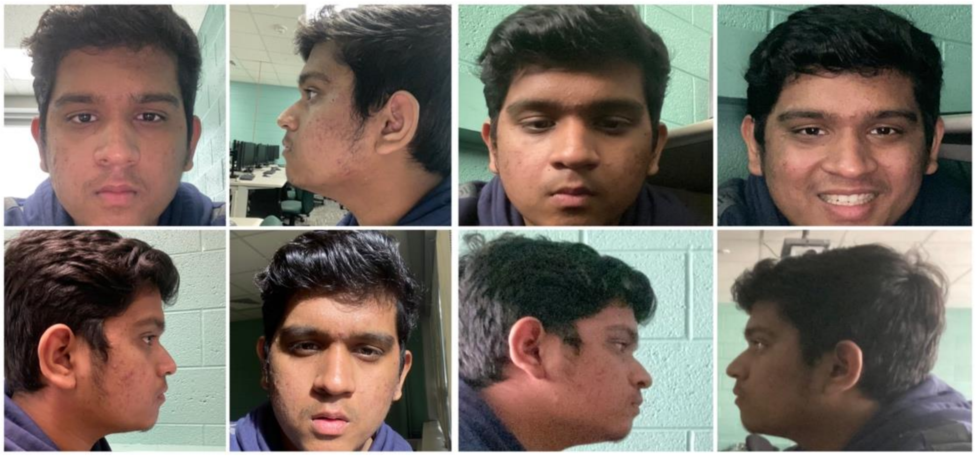
3. [10 points] Describe in detail the differences between a *VERIFICATION* system and an *IDENTIFICATION* system. You must state at least 4 differences. In addition, describe 1 example for each system.

Ans)

Verification	**Identification**
In verification the user claims and identity which the system verifies if its genuine claim or not. (One to One).	In identification the user doesn’t claim an identity instead the user identity is matches with the identities in the database. (One to N number of matches).
Verification helps in preventing unauthorized users from using authorized services.	Identification helps in preventing a user from having multiple credential records or enjoying many benefits under different names.
In verification if the input and template of the claimed identity have a high degree of similarity then it is accepted as genuine and if it rejected it is considered as impostor	Identification can be classified into positive and negative identification. In positive identification the user attempts to positively identify himself to the system without explicitly claiming an identity whereas in negative identification the user is hiding his true identity from the system.
In Verification the system answers the question “Are you who you say you are?”	In Identification the system answers the question “Are you someone who is known to the system?”
Example: Face id or fingerprints that you use to unlock your mobile device.	Example: It is used in police stations screenings to identify the people in the watchlist.

4. [10points] Use a webcam or a smartphone camera to capture 10 images of your face. The images must exhibit variations in facial pose (e.g., frontal face profile, side face profile), il- lumination (e.g., bright sunlight, low indoor lighting, partially illuminated face), expression (e.g., neutral, smiling, frowning), scale (e.g., close-up, at-an-arms-length), etc. Include these images in your report and describe, from your perspective, what type of facial features may be useful to successfully match these images. Justify your choice of features.

   Ans)



There are few types of facial features that may be useful to successfully match these images:

- Geometry of the face (eg: Jaw line structure)
- Dimensions of the teeth
- Iris
- Face recognition

5. You are given a set of scores corresponding to two modalities /matchers - fingerprint and hand. The fingerprint scores are *SIMILARITY-BASED*, while the hand scores are *DISTANCE-BASED*, i.e., *DISSIMILARITY-BASED*. The set of scores can be accessed here.

    (a) [2points]Howmanygenuineandimpostorscoresareavailableforthefingerprintmatcher and the hand matcher?

    Ans) Fingerprint genuine scores: 450
    Fingerprint impostor scores: 450

    Hand genuine scores: 450
    Hand impostor scores: 450

    (b) [4points]Whatarethemaximumandminimumscoresgeneratedbyeachmatcher?

    Ans) Finger genuine maximum score: 966.0

    Finger genuine minimum score: 0.0

    Finger impostor maximum score: 73.0

    Finger impostor minimum score: 1.0

    Hand genuine maximum score: 266.0

Hand genuine minimum score: 0.0

Hand impostor maximum score: 626.0

Hand impostor minimum score: 44.0

(c) [9points]Write a program that inputs a threshold value, η, for each matcher, the set of genuine scores, and the set of impostor scores, and outputs the False Match Rate (FMR) and False Non-match Rate (FNMR) at that threshold. Use this program to compute the FMR and FNMR for the following scenarios:

i. Fingerprint Matcher: $\eta = 45$

ii. Hand Matcher: $\eta = 45$

Ans) False Match Rate Similarity = 1.33 %
False Match Rate Dissimilarity = 0.67 %

False Non-Match Rate Similarity = 10.44 %
False Non-Match Rate Dissimilarity = 43.56 %