**Homework 1**

**Nicholas Shari**

**CSE 402 - Biometrics and Pattern Recognition**

**Instructor: Dr. Arun Ross**

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

**Total Points: 60**

**Note:**

**You are permitted to discuss the following questions with others in the class.**  **However, you *must* write up your *own* answers to these questions. Any indication to the contrary will be considered an act of academic dishonesty.**

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

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

**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.**

**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.**

**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?

* Continuous authentication is using biometric or behavioral attributes to verify the current user of the device is the owner or person authorized to use the device at frequent intervals during operation. This provides additional layers of security after an initial authentication is performed.
* Continuous authentication is becoming more necessary with mobile devices as they store more personal and sensitive data about their users. A common mobile device can store all of their owner’s passwords, credit card information, and biometric data such as face and fingerprint images. With continuous authentication during operation it would prevent someone from unlocking the device with a pin or password and accessing all stored data by locking the device when features such as gait, gestures, or facial recognition cannot be replicated.

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

* Continuous authentication
* Implicit authentication
* Active authentication
* Transparent authentication

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

* The most impairing limitation of explicit authentication such as passwords and PINs is the susceptibility to human error and effort. A PIN or password is only as secure as the person that creates or maintains it. If the password is easy to guess such as “password” or “123”, a device can easily be hacked. If someone chooses to write their pin on a sticky note that is on their desk; now their device is no longer secure.
* Explicit mechanisms can also be cumbersome to the user. If a user is prompted every 60 seconds to enter their PIN while watching a video they would be likely to be annoyed.

(d) Describe some of the biometric attributes that can be used for continuous authentication.

* Facial recognition. The front-facing camera can record an image of the user’s face for authentication. This can be spoofed with a photo of the person or a mask.
* Gestures. The device can record the stroke timing, length, angle, pressure, and width of a finger and authenticate the user.
* Gait. The device’s accelerometer and gyroscope can record how a user walks and use that to authenticate the user. Unfortunately an injured leg could throw off the pattern of how someone would usually walk.

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

* Facial recognition. This can be spoofed with a photo of the person or a mask.
* Gestures. Some applications require the user to use multiple fingers to perform operations such as zoom in and zoom out. This becomes more problematic to calculate. There are also no gestures if a user is watching a video for an extended length of time.
* Gait. Unfortunately an injured leg could throw off the pattern of how someone would usually walk.

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

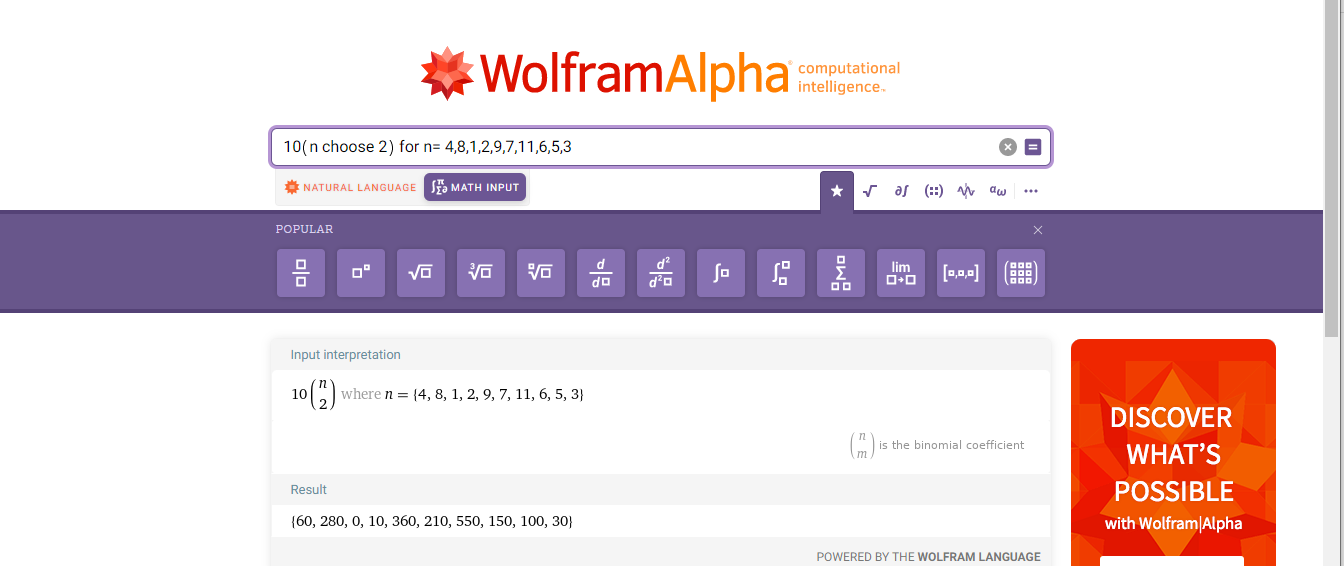
010 3

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.

Genuine Scores: N[binomial(m, 2)] N is Number of identities, m is samples per face.

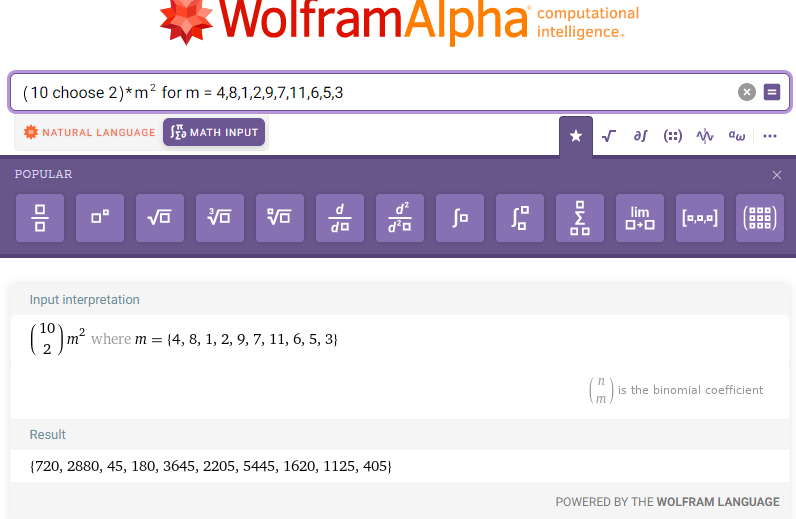
10 binomial(4, 2) + 10 binomial(8, 2)+ 10 binomial(1, 2)+10 binomial(2, 2)+10 binomial(9, 2)+ 10 binomial(7, 2)+ 10 binomial(11, 2)+ 10 binomial(6, 2)+ 10 binomial(5, 2) + 10 binomial(3, 2)

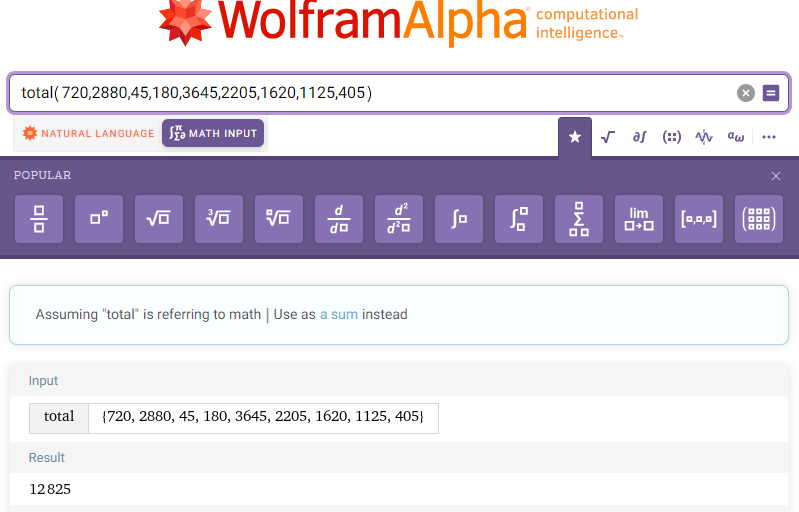
60 + 280 + 0 + 10 +360 + 210 + 550 + 150 + 100 + 30 = 1750



Imposter Scores: binomial(N, 2) m^2N is Number of identities, m is samples per face.

Total = 12,825





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.

1. Verification is one to one matching to determine if the person attempting to access a system is indeed that person. Identification is a one to many matching to compare if the accessing user is amongst a database of users to ensure they are authorized to use that system.
2. Verification requires a user to tell the system who they are. While identification is the system trying to recognize a user based on analysis.
3. Identification is generally slower because it has to check the gathered data against all entries.
4. Verification checks the entry against a template.

Verification: A person enters their PIN to prove they are the phone’s owner to unlock the phone.

Identification: A door is locked and uses a biometric scanner to control access. A person has to place their finger on a scanner to verify they are authorized access in the system.

4. [10 points] 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.

\*Pictures at the end of the report.

Features:

* Distance between the eyes.
  + This cannot be changed by changing your facial expression.
* Upper/lower lip width.
  + Mouse shapes are unique and vary between people.
* Distance from upper lip to the bottom of nose.
  + While smiling and from a side profile this distance does not change.
* Width/height of eyes.
  + The shape of an individual’s eyes can vary depending on if they are squinting or glaring. However the width of their eyes is unchanging.
* Distance from forehead to brow.
  + This distance is the same from a front and side profile.
* Distance from top of forehead to bottom of the chin.
  + This distance is the same from a front and side profile.
* Ear shape/length.
  + Front a side profile the shape of the ear is unique. Front a front profile the length of the ear cannot be changed by facial expression.
* Skin color.
  + Skin color can only vary throughout various lightings.
* Markings - moles, freckles, scars, tattoos
  + Distinguishing permanent marks are unlikely to change without surgery or makeup. These could be an easy “go or no go” metric.

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) [2 points] How many genuine and impostor scores are available for the fingerprint matcher and the hand matcher?

Fingerprint:

Genuine: 450

Imposter: 450

Hand Matcher:

Genuine: 450

Imposter: 450

(b) [4 points] What are the maximum and minimum scores generated by each matcher?

. Fingerprint:

Genuine: Max: 966 Min: 0

Imposter: Max: 73 Min: 1

Hand Matcher:

Genuine: Max: 266 Min: 0

Imposter: Max: 626 Min: 44

(c) [9 points] 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: *η* = 45

ii. Hand Matcher: *η* = 45

Fingerprint:

FMR: 0.013333333333333334

FNMR: 0.10444444444444445

Hand:

FMR: 0.9933333333333333

FNMR: 0.5511111111111111

Bibliography:

1. *Wolfram: Alpha: Making the world's knowledge computable*. WolframAlpha computational knowledge AI. (n.d.). Retrieved September 21, 2022, from https://www.wolframalpha.com/
2. Ross, A. (n.d.). Homepage - Michigan State University. Retrieved September 21, 2022, from https://d2l.msu.edu/d2l/le/content/1579304/viewContent/13173051/View
3. Jain, A. K., Ross, A. A., Nandakumar, K., & Wayman, J. (2011). *Introduction to biometrics*. Springer Science+Business Media.

