Graphical Password Authentication System

180170116005 - Vishvaa Chhatrara
180170116017 - Rutanshi Khambhatiya
180170116022 - Priya Naika
190173116018 - Harshil Ramanuj

Outline

- Work done till now
- The method we implemented
- Dataset used
- Presentation of the web-app
- Functions of the web-app
- Documents prepared
- Future work:

Work Done till now

Graphical Passwords

- Graphical password can be used as an alternative to text based (alphanumeric) password in which users click on images to set their passwords.
- Images are generally easier to be remembered than text and in Graphical password; user can set images as their password.
- Where it can be applied:
  - Workstations
  - Web login applications
  - Mobile Devices
  - ATM and Banking Transaction Apps.
- Categories:
  - Recognition Based Techniques
  - Recall Based Techniques
  - Cued Recall Based Techniques

7

Recognition based Authentication:

- A user is given a set of images and he has to identify the image he selected during registration.
- For example, Passfaces is a graphical password scheme based on recognizing human faces. During password creation, users are given a large set of images to select from. To log in, users have to identify the pre-selected image from the several images presented to him.

8

Recall based Authentication:

- A user is asked to reproduce something that he created or selected at the registration stage.
- For example, in the Passpoint scheme, a user can click any point in an image to create the password and a tolerance around each pixel is calculated. During authentication, the user has to select the points within the tolerance in the correct sequence to login.

9

Cued Recall:

- Cued Click Points (CCP) is an alternative to the PassPoints technique.
- In CCP, users click one point on each image rather than on five points on one image (unlike PassPoints). It offers cued-recall and instantly alerts the users if they make a mistake while entering their latest click-point.

Some known attacks

- Brute force search
- Dictionary attack
- Guessing
- Spyware
- Shoulder Surfing
- Social Engineering

Drawbacks of current scenario..

- It requires more storage space because of images.
- Registration and login process take too long time
- **Less resistant to shoulder surfing.**

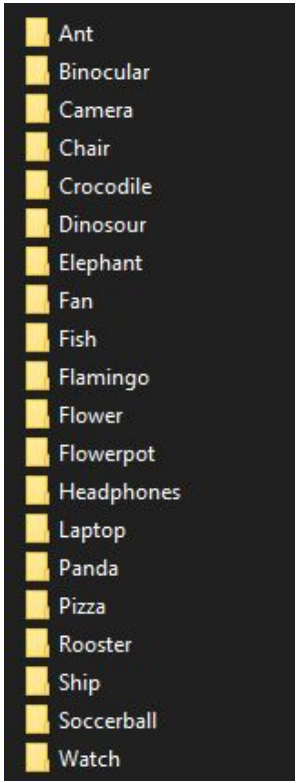
The method we implemented

- **Overview: Enter opposites**
  - At the time of registration user is asked to select the 3 categories out of given 8 categories of images(i.e. Cars, Pets, Fruits etc.)
  - At the login time user has to recall which categories he had selected. And Do NOT select that from given set of images having mixture of all categories.
  - This approach can confuse the shoulder surfer and would decrease the chances of success in attack.

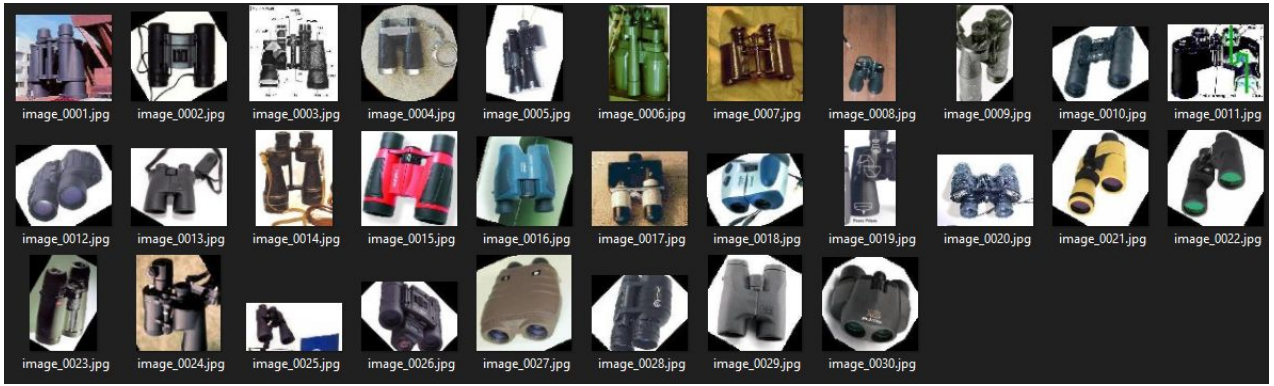
Continued...

- **Our Application:**
  - Increased choice categories from 8 to 20
  - Updated the number of choices from (3) to (3 to 5).
  - User Register his details like email and phone number and will register his choices of image categories.
  - The user moves to login and submits the images.
  - If entered images are correct, the page shows a “Success” message
  - Else if less number of images are selected, the page shows an “Incorrect number of images selected” message
  - Else if false images are selected, the page shows “Invalid choice of images” message
  -

Dataset used...



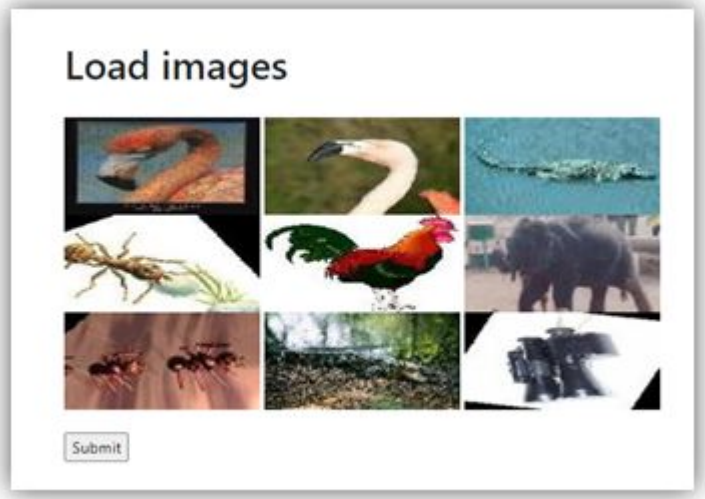
- As we can see in the picture, our dataset contains 20 folders of different bird/animal/fish/things (in common, objects) and each folder contains 30 images of a particular object.
- Thus, we have a total of 600 images in the dataset.
- The dimensions of images are not the same but for presenting on the app, they are resized to 200X100 pixels by the algorithm.



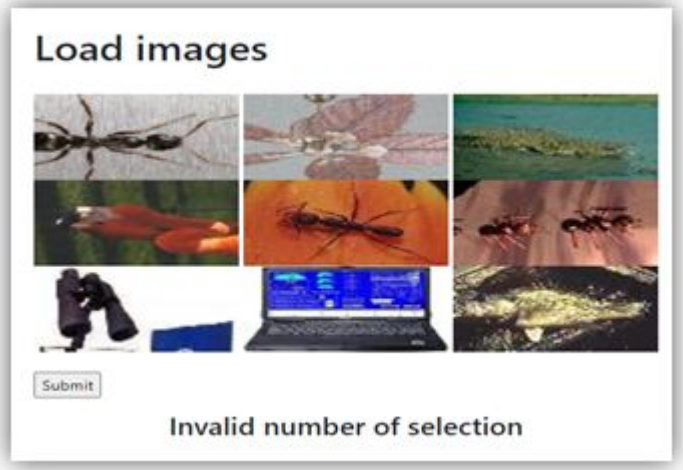
The UI of web-application

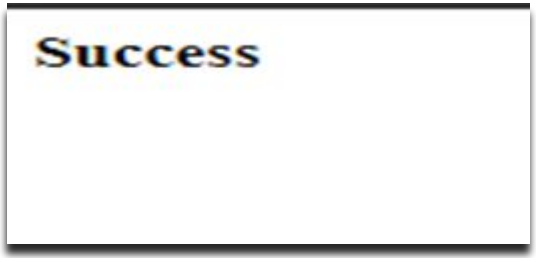
Registration phase

Login Phase



Success/Failed attempt:



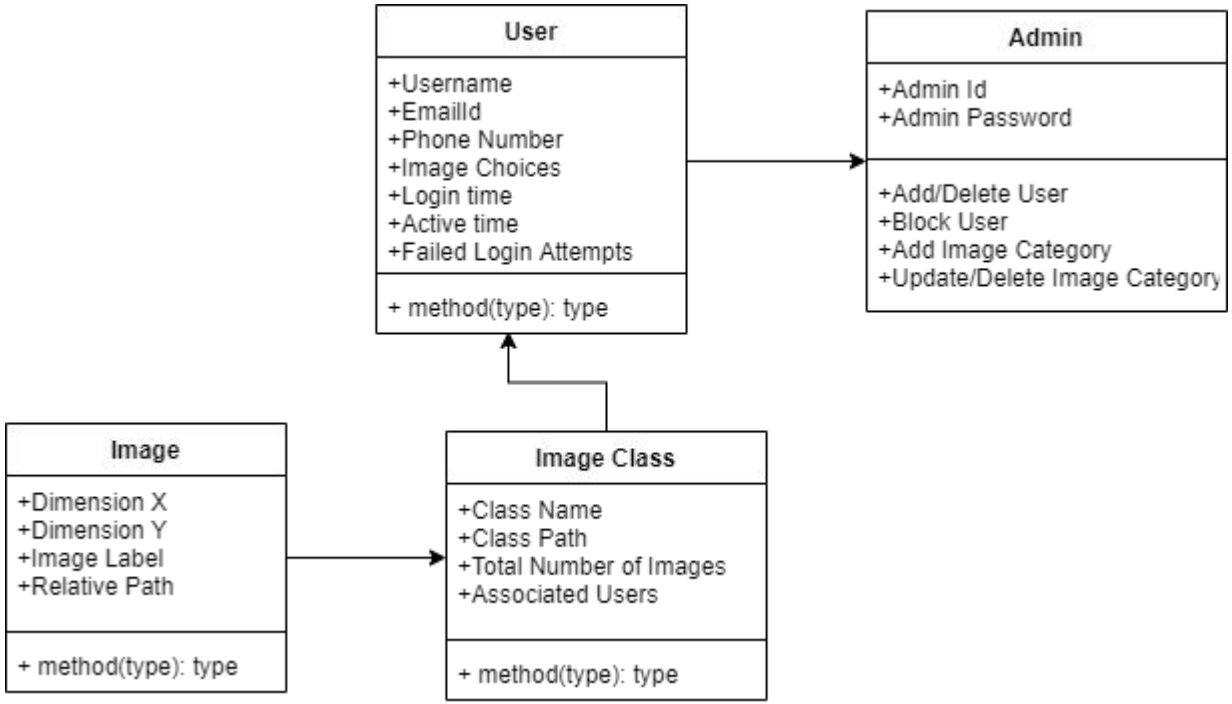


Functions of the webapp

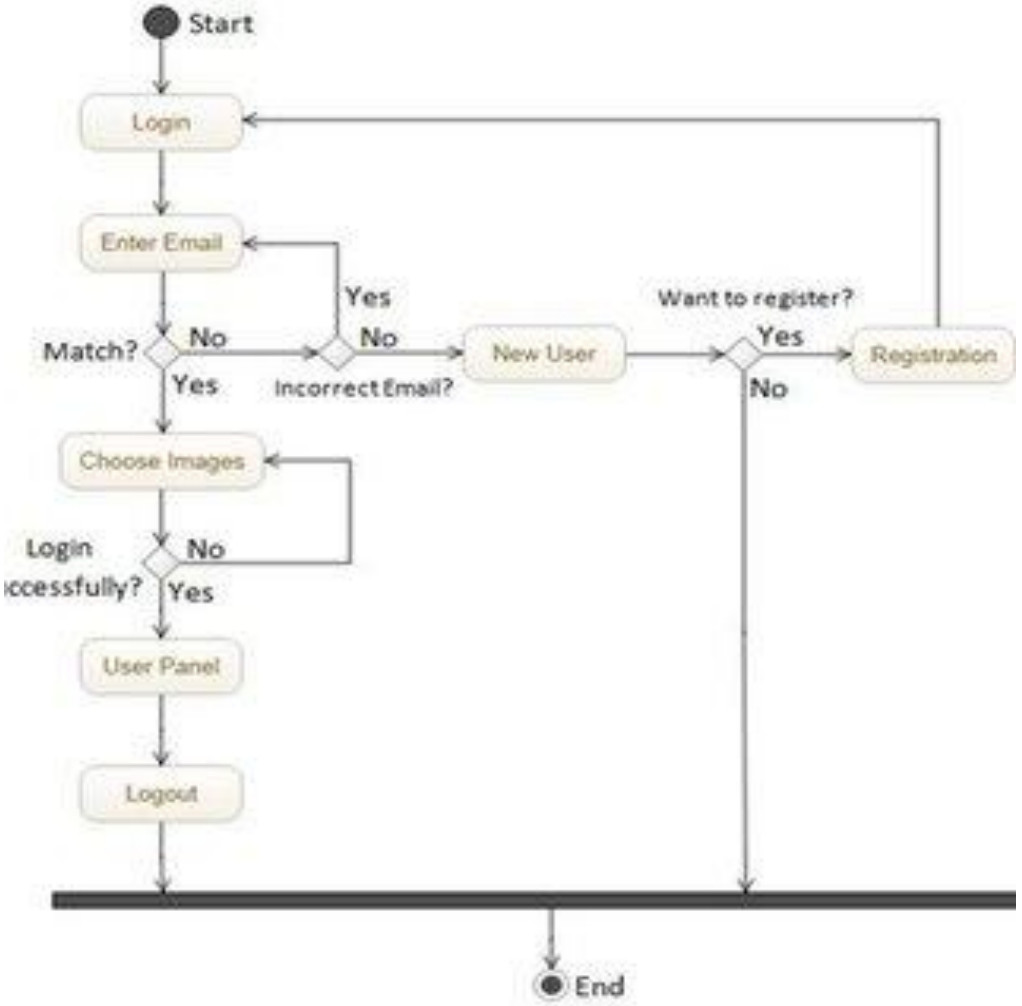
- Register Graphical Password
- User Verification
- Recovery Options
- Data Validation
- Quality Check
- Permissions/Accessibility to system

UML Diagrams

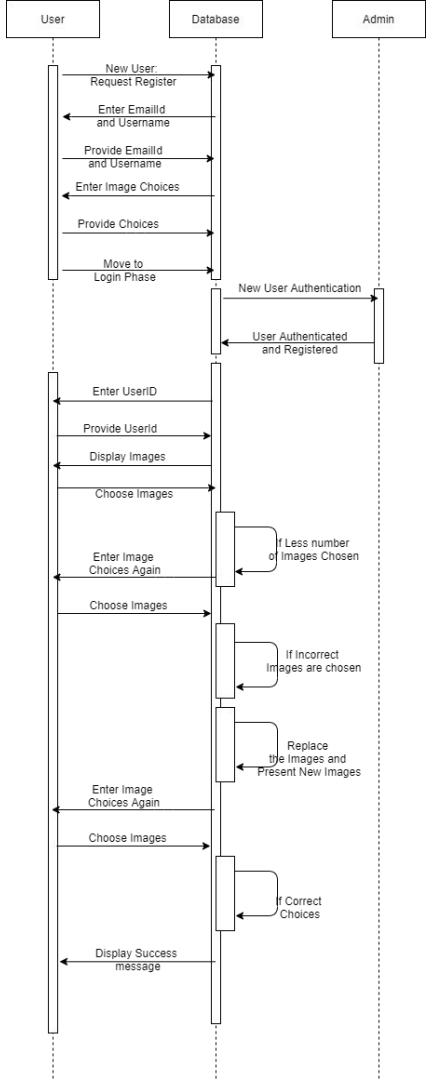
1. Entity Relationship Diagram



2. Activity Diagram



3. Sequence Diagram



4. Use Case Diagram:

Future Work

- Testing the app
- Improvement in UI
- Performance measurement of the app
- Password Recovery