

GRAPHICAL PASSWORDS: BEHIND THE ATTAINMENT OF GOALS

Project submitted in partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

BY

S JANAKI RAM

(19C95A0507)

V ROHITH

(19C95A0508)

V MANIKANTA

(19C95A0509)

Under the Esteemed guidance of

Mrs. Sree Lakshmi



Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE

(COLLEGE OF ENGINEERING)

(Approved by AICTE New Delhi, Permanently Affiliated to JNTU Hyderabad, Accredited by NAAC with 'A' Grade)

Bogaram (V), Keesara (M), Medchal District -501 301. – 11

2021 - 2022

HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE

(COLLEGE OF ENGINEERING)

(Approved by AICTE New Delhi, Permanently Affiliated to JNTU Hyderabad, Accredited by NAAC with 'A' Grade)

Bogaram (V), Keesara (M), Medchal Dist-501301.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



CERTIFICATE

This is to certify that the mini project entitled “**GRAPHICAL PASSWORDS: BEHIND THE ATTAINMENT OF GOALS**” is **being** submitted by **S JANAKI RAM (19C95A0507)**, **V ROHITH (19C95A0508)**, **V MANIKANTA (19C95A0509)**, in Partial fulfillment of the academic requirements for the award of the degree of Bachelor of Technology in “**COMPUTER SCIENCE AND ENGINEERING**” **HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE, JNTU Hyderabad** during the year 2021- 2022.

INTERNAL GUIDE

Mrs.R. SREELAKSHMI (M.Tech)

Assistant Professor

Dept. of Computer Science & Engineering.

HEAD OF THE DEPARTMENT

DR.B.NARSIMHA M.Tech, Ph.D.

Professor & HoD

Dept. of Computer Science & Engineering

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible, who's constant guidance and encouragement crowns all effort with success.

I take this opportunity to express my profound gratitude and deep regards to My Guide **Mrs. Sree Lakshmi, Assistant Professor**, Dept. of Computer Science & Engineering, Holy Mary Institute of Technology & Science for his / her exemplary guidance, monitoring and constant encouragement throughout the project work.

My special thanks to **Dr. B. Narsimha, Head of the Department**, Dept. of Computer Science & Engineering, Holy Mary Institute of Technology & Science who has given an immense support throughout the course of the project.

I also thank to **Dr. P. Bhaskar Reddy**, the **Honorable Director** of my college Holy Mary Institute of Technology & Science for providing me the opportunity to carry out this work.

At the outset, I express my deep sense of gratitude to the beloved **Chairman A. Siddarth Reddy** of **Holy Mary Institute of Technology & Science**, for giving me the opportunity to complete my course of work

I am obliged to **staff members** of Holy Mary Institute of Technology & Science for the valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of my assignment.

Last but not the least I thank **ALMIGHTY** and My **Parents**, and **Friends** for their constant encouragement without which this assignment would not be possible.

S JANAKI RAM

(19C95A0507)

V ROHITH

(19C95A0508)

V MANIKANTA

(19C95A0509)

DECLARATION

This is to certify that the work reported in the present project titled **“GRAPHICAL PASSWORDS: BEHIND THE ATTAINMENT OF GOALS”** is a record of work done by me in the Department of Computer Science & Engineering, Holy Mary Institute of Technology and Science. No part of the thesis is copied from books/journals/internet and wherever the portion is taken, the same has been duly referred in the text the reported are based on the project work done entirely by me not copied from any other source.

S JANAKI RAM

(19C95A0507)

V ROHITH

(19C95A0508)

V MANIKANTA

(19C95A0509)

CONTENTES

Name of chapter	page No.
1. ABSTRACT	
INTRODUCTION.....	1 - 2
2. LITERTURE SURVEY	
PROPOSED SYSTEM.....	3 - 4
EXISTING SYSTEM.....	4 – 10
3. SYSTEM ANALYSIS	
SOFTWARE REQUIREMENTS.....	11
HARDWARE REQUIREMENTS.....	11
4. SYSTEM DESIGN	
SYSTEM ARCHITECTURE.....	12
5. IMPLEMENTATION	
ENVIRONMENT SETUP.....	13
SOFTWARE DESCRIPTION.....	13
SAMPLE CODE.....	13 – 20

6. SYSTEM TESTING

TESTS.....	21 – 24
------------	---------

7. RESULTS & SCREEN SHOTS.....25

8. CONCLUSION.....33

9. BIBLIOGRAPHY.....34

LIST OF FIGURES

Figure Names	Page no.
REGISTRATION PHASE.....	6
DERIVATION OF USER AND SYSTEM SHARES.....	7
BLURRED VERSION OF IMAGES.....	8
LOGIN PHASE.....	9
USERID AFTER COMBINING USER AND SERVER SHARES.....	9
LOGIN PAGE WITH BLURED IMAGE SET.....	10
SUBSEQUENT LOGIN SESSION COMPARING PREVIOUS ONE WHICH CONATION EIGHT REPEATED IMAGES	21
START PHP SERVER.....	21
BROWSER.....	22
SIGNUP PAGE.....	22
SELECT PASS IMAGES.....	23
SIGN UP SUCCESSFUL.....	23
LOGIN PAGE.....	24
PASS IMAGE PAGE.....	24
WORKING OF SERVER.....	29
LOGIN SUCCESSFUL.....	30
USER DATA STORED AS ENCRYPTED AND STORED IN DATA BASE.....	30

ABSTRACT

Graphical authentication methods have emerged as an alternative to the conventional authentication methods over the past couple of decades.

One of the most popular among types of graphical authenticational methods is recognition-based authentication, where the user taps on pass images from one or more challenge set of images in order to authenticate.

The study of existing graphical authentication systems shows that several of them compromise their security while making the method simpler, which could lead to perpetration of numerous attacks like guessing, hidden camera, smudge, shoulder surfing, and many other.

Furthermore, a few of them sacrifice performance while targeting security alone.

Yet, this paper proposes a new method that resists the aforementioned attacks with good performance, while preserving the benefits of graphical passwords such as ease of use and increased memorability.

1. INTRODUCTION

Text based passwords are widely held authentication schemes until date for the reason of user familiarity. The problem with this system seen in the form of short passwords picking and storing them at vulnerable locations that degrades security further. Conversely, the long passwords are not easy to remember. Thus, the users tend to use the same passwords for multiple accounts that can put all such accounts under risk when associated password is compromised. Studies have shown that graphical passwords are better alternative to text-based passwords from the perspective of memorability and usability. Psychologists have shown that images are more memorable to humans than text based on recognition and recall grounds. Consequently, graphical password authentication systems have gained attention ever since its introduction in 1996 due to aforementioned advantages.

Graphical passwords are categorized into recognition-based, pure recall-based, and cued-recall. Recognition based authentication system involves identification of the true images, which were chosen at the time of registration. However, this scheme can be circumvented by using phishing attacks in which users are tricked into taking screenshots of their passwords. Other usability drawbacks of this scheme are to scan multiple images to identify a few preselected images for the password, which is considered as a time-consuming process. In pure-recall based authentication system, users have to reproduce or draw something as their password. Pure-recall based schemes address the drawbacks of recognition-based schemes but are prone to errors when a stylus is not used. The recall-based systems are less vulnerable to dictionary, brute-force and social engineering attacks than text-based passwords because imitating human inputs by automatically generating mouse motions is difficult. However, the problem with pure-recall based schemes is the users can hardly remember the sequence of drawing after a period. Additionally, it is challenging to reproduce the drawing same as the original password. Cued-recall authentication involves predetermined image presented to the user, and user should tap on one or more predetermined positions of the image in a predetermined order. The use of predefined click objects required simple, artificial images, for example cartoonlike images, instead of complex and real-world scenes. The user always tends to choose the hotspot of the image, which can be easy for attacker to guess.

There are also several attacks possible on these graphical password schemes. Brute-force attack stands first in the row in which user tries every possible combination of images in order to obtain the correct password. Educated guess attacks make attacker job even simpler under the assumption of attacker possessing prior knowledge about the user.

In addition, sniffing attacks are possible when data are transmitted over the public channels that is, if the data packets are not encrypted. Phishing attack is possible by disguising as a trustworthy entity in a communication. Hidden camera attacks are likely to occur if the attacker uses a spy camera and records user personal information. Shoulder surfing attacks are also feasible in which attackers try to obtain passwords and confidential data by looking over the victim's shoulder. A graphical password scheme must be designed while bearing in mind all aforesaid aspects.

2. LITERATURE SURVEY

INTRODUCTION

Several researchers have proposed numerous graphical based authentication schemes to defend quite a few of previously mentioned attacks. Our and others analysis of these authentication schemes exhibited several severe flaws. We also have noticed a few good approaches to strengthen the authentication scheme as furnished below.

Hayashi et al proposed a scheme in which images are distorted to resist the educated guess attacks. Sun et al conducted research on authentication scheme against shoulder surfing attacks and proposed a scheme using a login indicator that is generated randomly for every pass image and is useless after terminating the session. The login indicator offered better security against shoulder surfing attacks. It also offered no indication even if multiple camera-based attacks are performed.

Ordean et al put forward a recognition-based scheme while performing small modifications to images intending to resist attacks. The purpose is to create temporary image sets indistinguishable from one another. Using these image sets, passwords become valid for short periods and only with binding image set. However, replay and brute-force attacks are still possible on this method. Additionally, computations on server-side increase as the authentication image sets changes over multiple login attempts.

Gao et al proposed a graphical authentication scheme aiming to protect against shoulder surfing attacks. During authentication phase of this scheme, user must recognize his/her pass-images and draw a curve to orderly cross them. The curve thus passes through both pass images and other random images to confuse the attacker. This forces the user to remember the order, which was selected by him at the time of registration phase.

PassBYOP is another graphical authentication scheme that replaces the static digital images typically used in graphical password systems with personalized physical tokens in the form of digital pictures displayed on a physical user-owned device such as a mobile phone. Users present these images to a system camera and then enter their password as a sequence of selections on live video of the token. This authentication scheme is resistant to security attacks; however, it has limitations in terms of space and usability.

The paper has conducted a wide range survey in which different graphical authentication schemes including draw what you drew before, pick from a group, observation resistant picking from a group, pick a position, and so on were well deliberated. The mentioned authentication schemes of this paper have followed the designs such as Loci metrics, Draw metrics, and Search metrics. The security discussion has reflected the trade-off between guess ability and observability.

Karen et al proposed a high-end graphical authentication scheme. In order to enhance the security and effectiveness, the author combined four key features such as blurring, rotation, image resizing, and sequence in the framework. This scheme is flexible as the user is allowed to choose his own blur index, angle of rotation, sequence of the pass images, and the extent of image resize. Most of the users indicated that this system is better for end users but not for high-end system, and the difficulty in terms of usability is intermediate according to them. Author also calculated the complexity of guessing the password by using different combinations of the features.

Shamir in his paper worked on the concept of visual cryptographic technique that allows visual information to be encrypted in such a way that decryption can be done just by sight-reading. In this type of cryptography, the encryption of original image is derived into two images by converting every pixel into pattern that looks like gray or noise. Authors also used OCR algorithm that showed various problems during development phase, which becomes a drawback though they minimized the computations by using visual cryptography.

Amalarethinam and Sai Geetha proposed public key cryptographic technique, which uses the concept of magic rectangle. During encryption, the selected image is converted into many blocks, and each block is replaced with the value of the magic rectangle. Control parameters can be randomly selected by the user himself and the image is being encrypted with existing symmetric key algorithms. The major drawback is that if the file size increases, the time for encryption and decryption also increases.

Miyachi et al proposed a graphical authentication scheme, which is difficult to steal original pass-image by using characteristics of human vision system. The author combined low frequency components of a decoy picture with high frequency components of a pass-image, which makes easy for legitimate users to recognize the pass-image in the blended image, and makes it difficult for shoulder surfing attacks. They deployed discrete wavelet transform to blend a decoy image and a pass-image.

The existing authentication systems were confined to address a few of the attacks among hidden camera, shoulder surfing, educated guess, brute force, sniffing, and phishing attacks. In addition, the current graphical authentication systems are more complex and targeted only towards a few categories of users like educated. These systems are more costly because they also include a special hardware in their experimental setup. The literature review plainly demonstrates a trade-off between security and performance. However, a graphical authentication system is said to be ideal only when it balances both the key features: security and performance. Henceforth, we intend to propose an efficient and user-friendly graphical authentication scheme with a negligible cost.

EXISTING SYSTEM

- The existing authentication systems were confined to address a few of the attacks among hidden camera, shoulder surfing, educated guess, brute force, sniffing, and phishing attacks.
- In addition, the current graphical authentication systems are more complex and targeted only towards a few categories of users.
- These systems are more costly because they also include a special hardware in their experimental setup.

DISADVANTAGES OF EXISTING SYSTEM

- Easy/Short passwords can be Hacked.
- long passwords/Strong password hard be remembered.
- Remembering Multiple Passwords is hard.
- Same password for multiple account, where multiple account may get in risk.
- Problems with passwords that needs to be continuously changed.
- Security vs. Ease-of-Use for Password.
- Shoulder Surfing Attack.

PROPOSED SYSTEM

The proposed scheme follows recognition-based techniques while integrating some of the finest concepts such as 5×5 grid, visual cryptography, distortion of images, and an email-id for recovery. In general, user-id plays a major role in graphical authentication because when user enters his user-id, a set of images are forwarded to the user from which he/she must choose four pass images in order to authenticate in subsequent logins.

In the proposed system we use images along with the password to overcome the problem which arises because of sharing and selection of weak passwords. Hence the system aims to achieve following:

- Authentication should not be based on precise recall of password.
- Make it difficult to share or write passwords.
- Provide good user experience.

Also, it's a proven fact that human user recognizes images faster as compared to recall of words. Standing shows that people can recognize images in spite of distracters and can retain over a period of time.

2.2.1 *Registration phase*

- *Step R1.* As shown in Figure 1, the registration phase obtains the details of users such as user-id, email-id, nationality, age, country, religion, profession, and gender.
- *Step R2.* Upon submitting the required information, user-id is converted into two images by using the concept of visual cryptography as shown in Figure 2 . One among these two images is sent to the user that is named as user share and the other one named as server share that is stored in the database for further use.

- *Step R3.* A 5×5 -image grid is now displayed to the user from which he/she chooses the pass images. The 25 images displayed are quite opposite to the details provided by the user with an objective to bring down the probability of guessing the pass images. Once the user taps the images, the distorted version of the same is revealed as these distorted images are used to authenticate in the subsequent login phases as presented in Figure 3.

Sign Up

Please fill in this form to create an account.

Email id	<input type="text" value="Enter Email"/>
User id	<input type="text" value="Enter userid"/>
Age	<input type="text" value="Enter age"/>
Gender	<input type="text" value="Enter gender"/>
Country	<input type="text" value="Enter country"/>
Religion	<input type="text" value="Enter religion"/>
Profession	<input type="text" value="Enter profession"/>

Figure 1
Registration page

rohith123

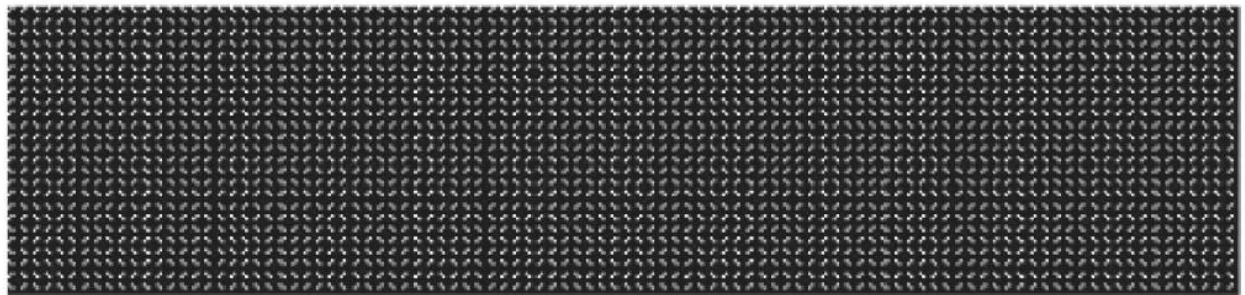
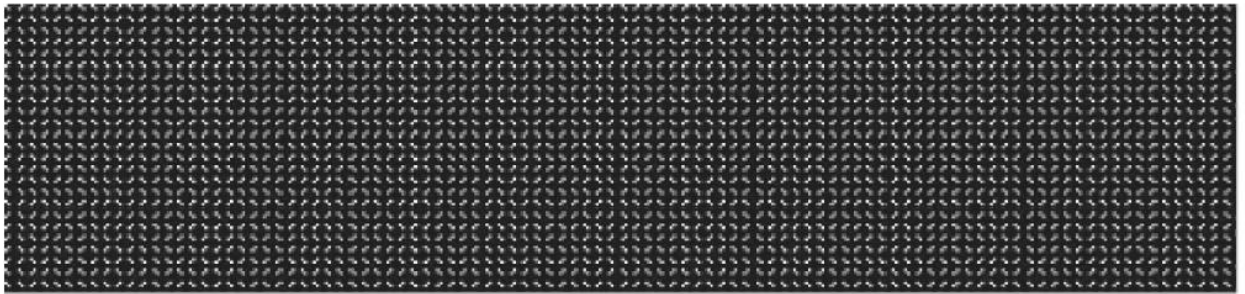


Figure 2

Derivation of user and system shares

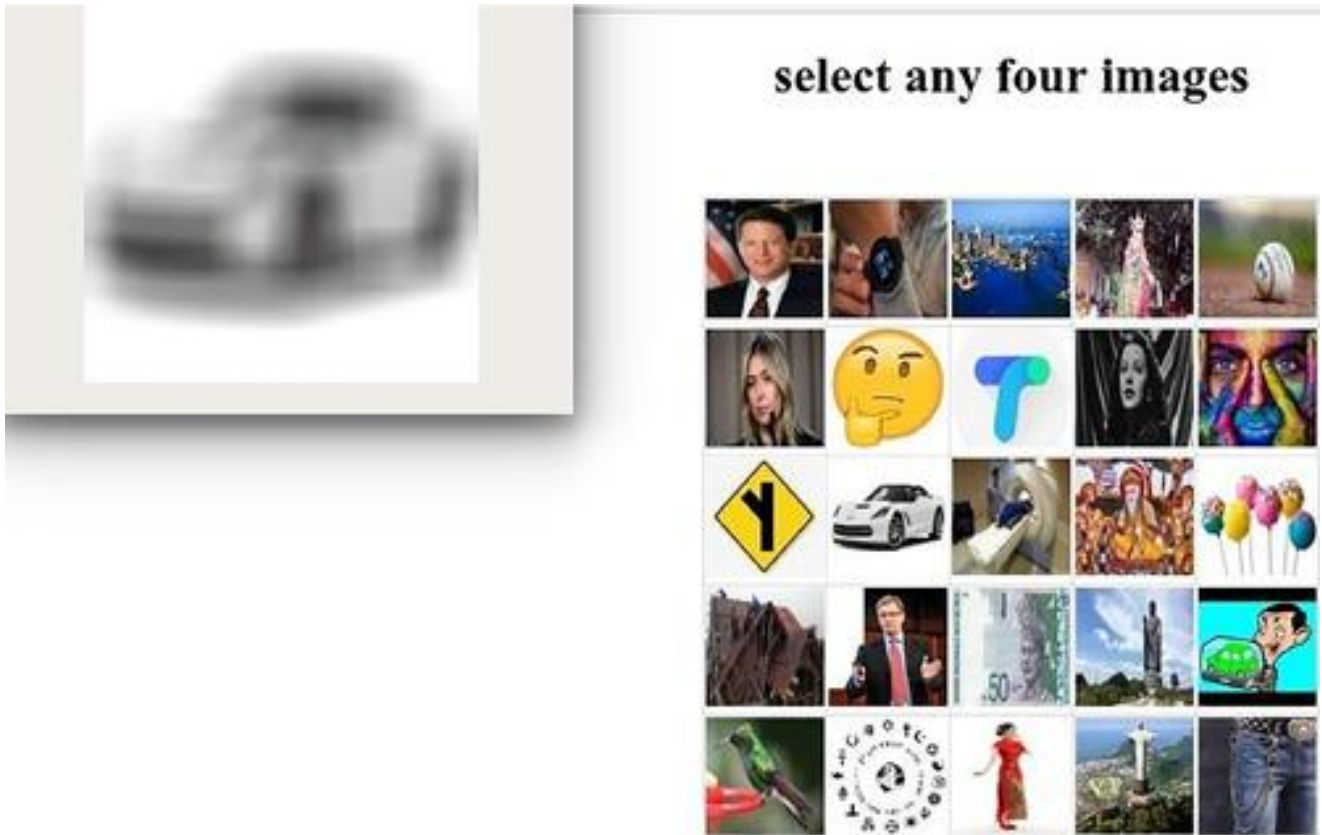


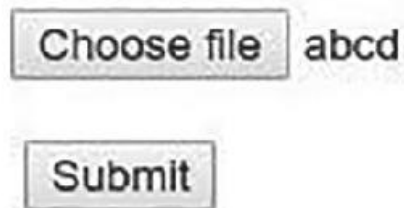
Figure 3
Blurred version of image

2.2.2 Login and authentication phase

- *Step L1.* During the login phase as shown in Figure 4, the user share must be submitted in order to display the user-id after combining both user share and server share as shown in Figure 5. User now can ensure the legitimacy of the site and continue the further process.
- *Step L2.* After the user ID appears, a distorted 5×5 -image grid displays including the pass images and random images as shown in Figure 6. The random images are the images chosen in accordance to the given details during registration. User is expected to tap the pass images for successful authentication. If the first attempt fails, another chance is given with the same image grid to prove his/her legitimacy. If the second attempt fails, the account will be locked for 5 hours and an email mentioning the same will be sent to user.
- *Step L3.* During the next login session, random images include eight images appeared during previous login along with four pass images as shown in Figure 7. This approach is deployed to lower the probability of guessing pass images even if attacker records the previous login session and keeps the record of images shown in the grid.

- *Step L4.* Another significant point to be noticed in the proposed scheme is no image is highlighted when user clicks the images during login phase in order to prevent shoulder surfing and hidden camera-based attacks. The user can also reselect the images if he/she has selected the wrong pass images.

upload your share to login



A login form interface. It consists of a button labeled "Choose file" followed by a text input field containing the text "abcd". Below this is a button labeled "Submit".

Figure 4
Login phase

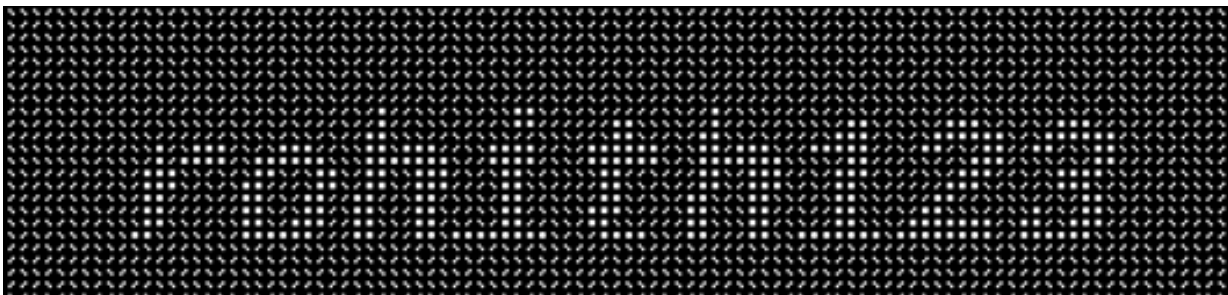
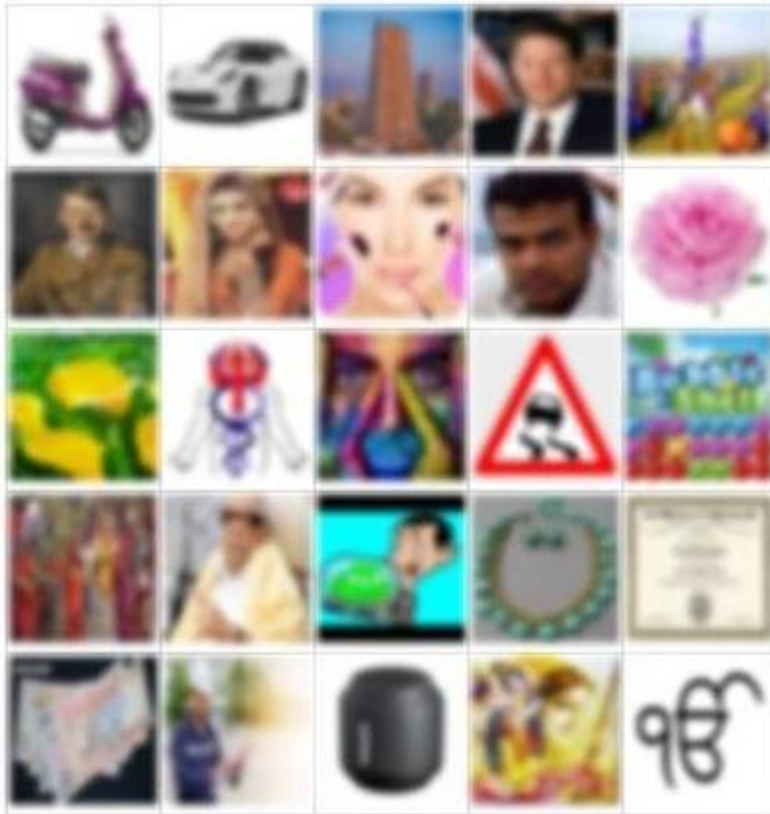


Figure 5
User ID after combining user and server shares

enter your pass images



RE-SELECT IMAGES

Figure 7

Subsequent login session comparing previous one which conation eight repeated images

3.SOFTWARE REQUIREMENTS SPECIFICATIONS

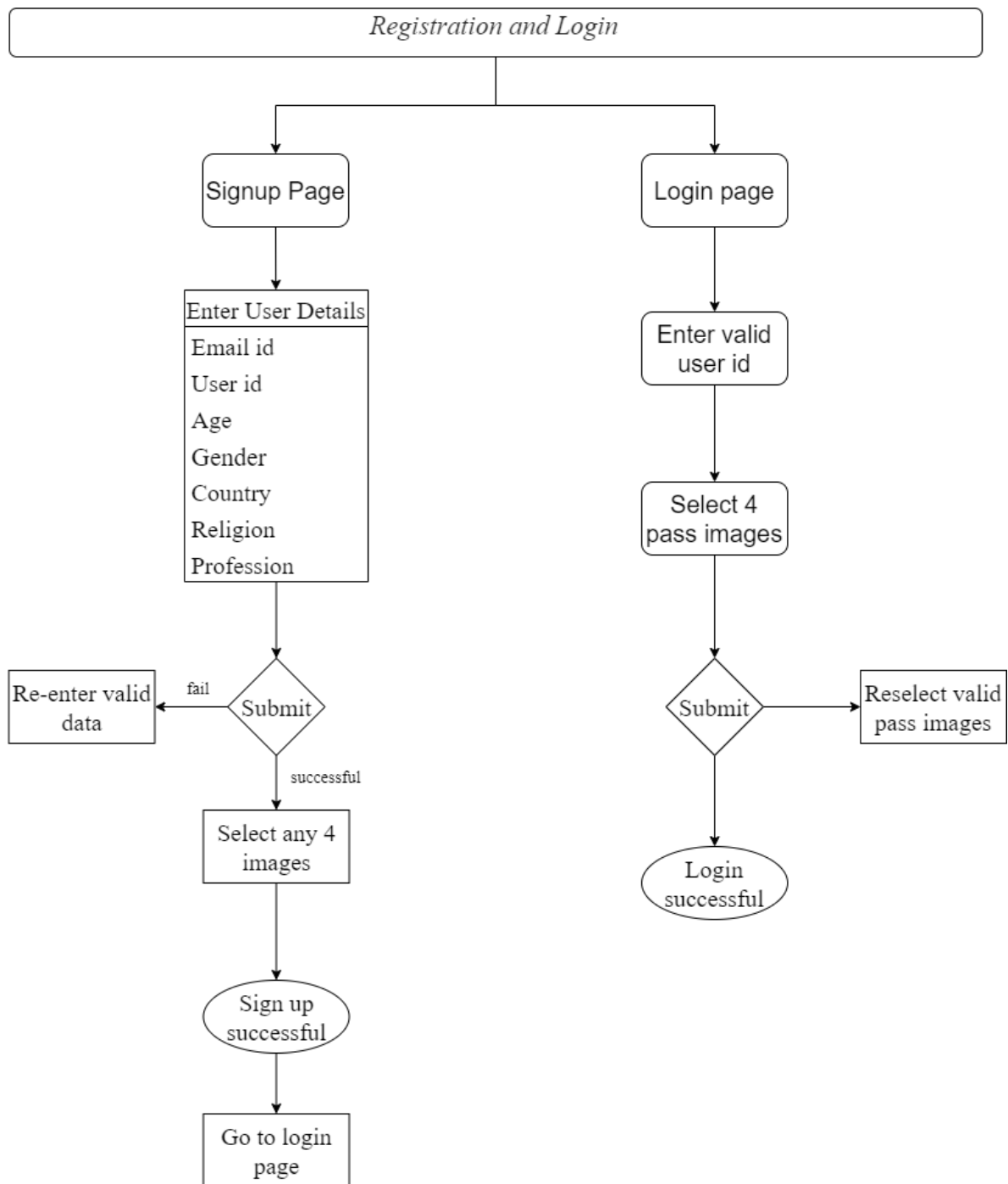
3.1 SOFTWARE REQUIREMENTS:

Operating system	:	Windows 10.
Coding Language	:	Python, HTML, PHP, JS
Editor	:	VS CODE

3.2 HARDWARE REQUIREMENTS:

System	:	Intel i3 Core, 5th gen
Hard Disk	:	80 GB.
Monitor	:	14'' or 15'' LED/LCD
Input Devices	:	Keyboard, Mouse
Ram	:	8 GB

4.SYSTEM DESIGN



5. IMPLEMENTATION

Environmental Setup:

- we need to Install PHP server in system.
- After installing set the path of php in environmental variables.

Start server:

- Open command prompt.
- Change directory where project file is stored.
- Start PHP server using “php -S localhost:8000” command.
- Server started now run local web page on any web page.

Browser:

- Open any browser.
- Search <http://localhost:8000/>.
- Test your web page.

Sample code: first page

```
<!DOCTYPE html>
<html lang="en">
<meta charset="utf-8"/>
<head>

<title> VC </title>

</head>
```

```

<body>

<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js"></script>

ob_start();
passthru('/usr/bin/python2.7 /home/Rohith/cns/project/overlap.py');
$output = ob_get_clean();
<!--
<form action="phpf.php">
  <input type="submit" value="click on me!">
</form>
<script src="vc.js"></script>-->

</body>
</html>

```

Sample code: signup page

```

<!DOCTYPE html>
<html lang="en">
<meta charset="utf-8"/>
<head>

<title> sign up </title>

</head>

<style>

```

```
body {font-family: Arial, Helvetica, sans-serif;}
* {box-sizing: border-box}
```

```
/* Full-width input fields */
```

```
body {font-family: Arial, Helvetica, sans-serif;}
* {box-sizing: border-box}
```

```
/* Full-width input fields */
```

```
input[type=text], input[type=password] {
    width: 50%;
    padding: 15px;
    margin: 5px 0 22px 0;
    display: inline-block;
    border: none;
    background: #f1f1f1;
}
```

```
input[type="number"], input[type=number] {
    width: 50%;
    padding: 15px;
    margin: 5px 0 22px 0;
    display: inline-block;
    border: none;
    background: #f1f1f1;
}
```

```
input[list="genders"], input[type=text] {
```

```
width: 50%;  
padding: 15px;  
margin: 5px 0 22px 0;  
display: inline-block;  
border: none;  
background: #f1f1f1;  
}
```

```
input[list="countries"], input[type=text] {  
    width: 50%;  
    padding: 15px;  
    margin: 5px 0 22px 0;  
    display: inline-block;  
    border: none;  
    background: #f1f1f1;  
}
```

```
input[list="religions"], input[type=text] {  
    width: 50%;  
    padding: 15px;  
    margin: 5px 0 22px 0;  
    display: inline-block;  
    border: none;  
    background: #f1f1f1;  
}
```

```
input[list="professions"], input[type=text] {  
    width: 50%;  
    padding: 15px;
```



```
margin: 5px 0 22px 0;
display: inline-block;
border: none;
background: #f1f1f1;
}
```

```
input[type=text]:focus, input[type=text]:focus {
  background-color: #ddd;
  outline: none;
}
```

```
hr {
  border: 1px solid #f1f1f1;
  margin-bottom: 25px;
}
```

```
.button {
  background-color: #4CAF50;
  border: none;
  color: white;
  padding: 15px 32px;
  text-align: center;
  text-decoration: none;
  display: inline-block;
  font-size: 16px;
}
```

```
.wrapper {
```

```

    text-align: center;
}

.button {
    position: absolute;

}
</style>
<body>

<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js"></script>

<form action="phpf.php" style="border: 1px solid #ccc" method="POST">
    <div class="container" align="center">
        <h1>Sign Up</h1>
        <p>Please fill in this form to create an account.</p>
        <hr>

        <label for="email"><b>Email id</b></label>
        <input type="text" placeholder="Enter Email" name="email" autocomplete="off" required>
        <br>

        <label for="uid"><b>User id</b></label>
        <input type="text" placeholder="Enter userid" name="uid" autocomplete="off" required><br>

        <label for="age"><b>Age</b></label>
        <input type="number" placeholder="Enter age" name="age" autocomplete="off" min="1"
max="99"
onKey="if(this.value>99){ this.value='99';}else if(this.value<0){ this.value='0';}" required><br>

```

```
<label for="gender"><b>Gender</b></label>
```

```
<input list="genders" placeholder="Enter gender" name="gender" autocomplete="off"
required><br>
```

```
<datalist id = "genders">
```

```
<option value = "male">
```

```
<option value = "female">
```

```
</datalist>
```

```
<label for="country"><b>Country</b></label>
```

```
<input list="countries" placeholder="Enter country" name="country" autocomplete="off"
required><br>
```

```
<datalist id = "countries">
```

```
<option value = "america">
```

```
<option value = "australia">
```

```
<option value = "brazil">
```

```
<option value = "china">
```

```
<option value = "denmark">
```

```
<option value = "egypt">
```

```
<option value = "india">
```

```
<option value = "japan">
```

```
<option value = "malaysia">
```

```
<option value = "russia">
```

```
</datalist>
```

```
<label for="religion"><b>Religion</b></label>
```

```
<input list="religions" placeholder="Enter religion" name="religion" autocomplete="off"
required><br>
```

```
<datalist id = "religions">
```

```
<option value = "buddhism">
```

```

    <option value = "christian">
    <option value = "hindu">
    <option value = "islam">
    <option value = "sikhs">
</datalist>

<label for="profession"><b>profession</b></label>

<input    list="professions"    placeholder="Enter    profession"    name="profession"
autocomplete="off" required><br>

<datalist id = "professions">
    <option value = "doctor">
    <option value = "engineer">
    <option value = "lawer">
    <option value = "police">
    <option value = "student">
    <option value = "teacher">

</datalist>

<div class="clearfix">
<div class="wrapper">

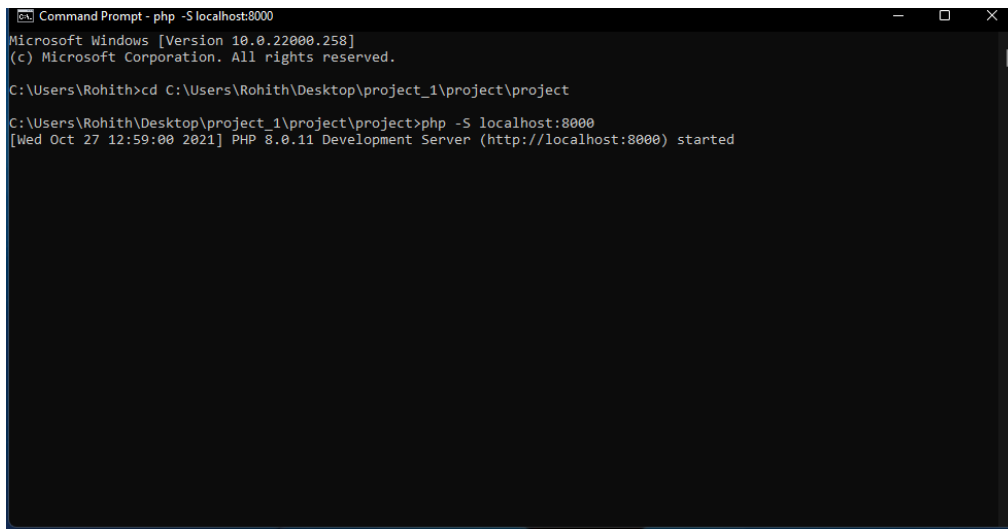
    <button type="submit" class="button">submit</button>
</div>
</div>
</div>
</form>
</body>
</html>

```

6. SYSTEM TESTING

Start server:

- Open command prompt
- Start php server using “php -S localhost:8000” command



```
Command Prompt - php -S localhost:8000
Microsoft Windows [Version 10.0.22000.258]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Rohith>cd C:\Users\Rohith\Desktop\project_1\project\project
C:\Users\Rohith\Desktop\project_1\project\project>php -S localhost:8000
[Wed Oct 27 12:59:00 2021] PHP 8.0.11 Development Server (http://localhost:8000) started
```

Figure 8: Start php server

Browser:

- Open any browser and search “<http://localhost:8000/>”.

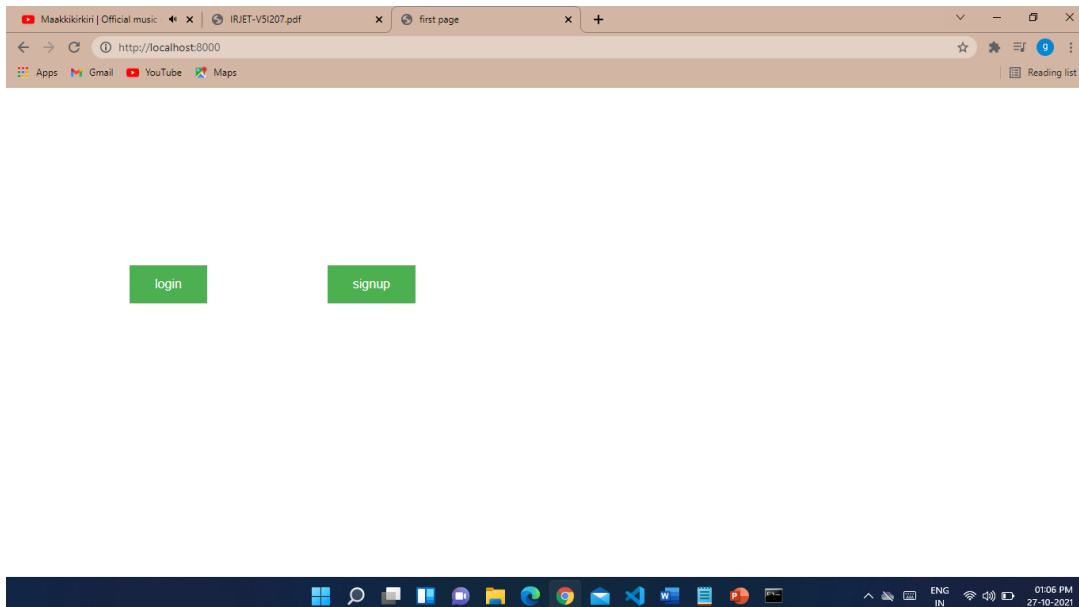


Figure 9: Google chrome browser

Sign Up

Please fill in this form to create an account.

Email id Enter Email

User id Enter userid

Age Enter age

Gender Enter gender

Country Enter country

Religion Enter religion

profession Enter profession

Figure 10: Sign up page

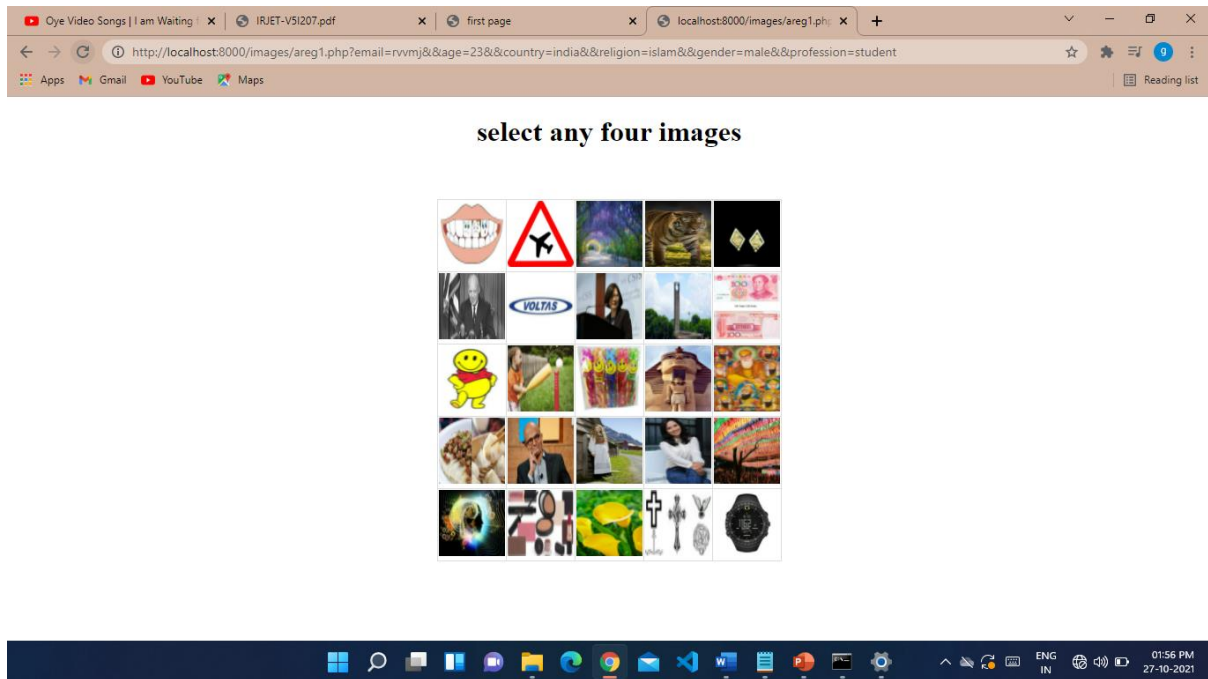


Figure 11: Select pass images

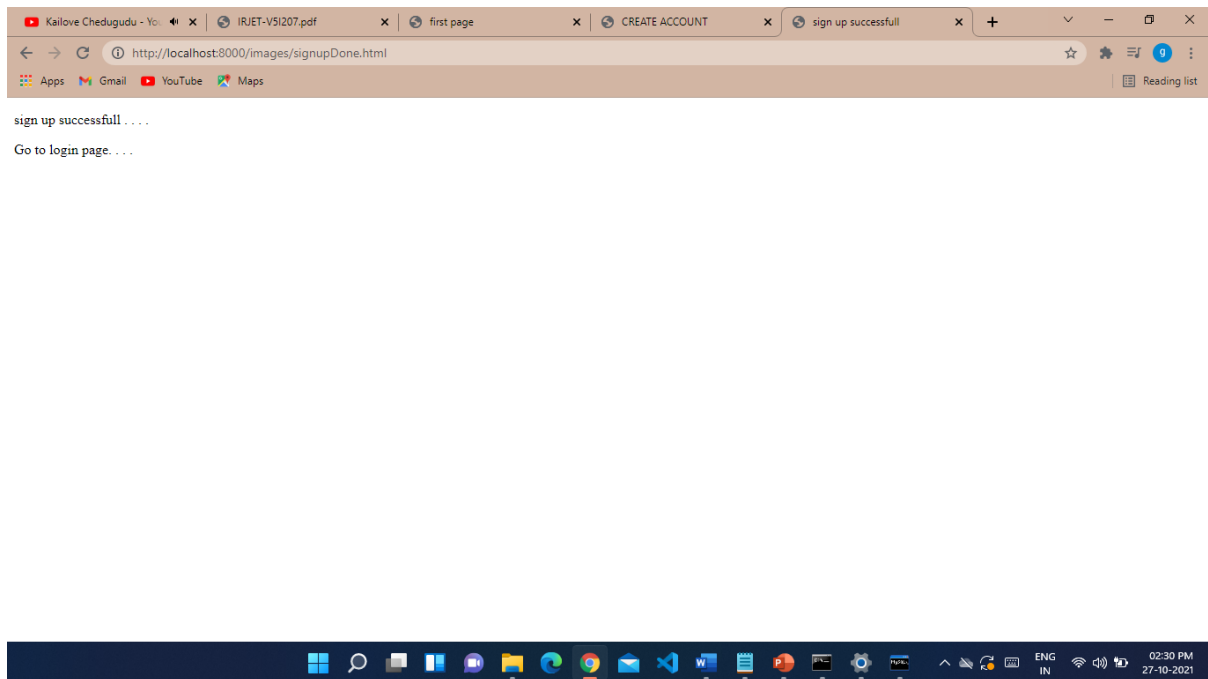


Figure 12: Sign up successful

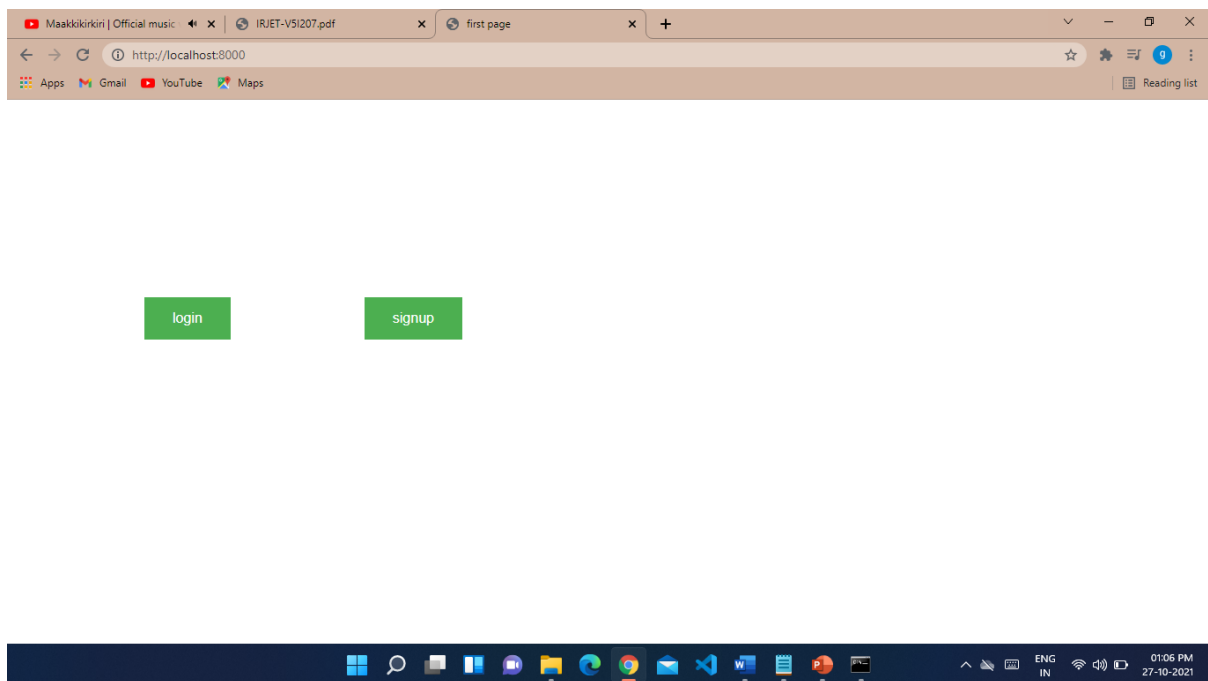


Figure 13: Login page

7. RESULTS AND SCREENSHOTS

7.1 Dataset description

Image dataset plays a vital role in any recognition based graphical authentication system. As the password comprises of images, the type of images to be displayed to the user should be considered with utmost care. In the registration step of the proposed system, the details of the user like country, age, profession, gender, and religion are collected. The image dataset may contain the images related to user provided details category. In addition to those images, a few more images irrespective of user details are also added to the dataset in order to introduce randomness in images set. Our dataset consists of 3000 images of different categories as described below.

- *Country dataset:* Most of the countries from all the continents are considered. Each country contains images that include human faces, places, monuments, dressing style, national flag, currency popular personalities, and politicians.
- *Religion dataset:* This dataset includes highly practised religions across the world. Each religion contains images including God and goddesses' images, their festivals, and mythological symbols used by respective religion.
- *Age dataset:* Based on the category of customers age, different images are presented to them. These categories include sections such as kids, teenagers, youth and adult. Kids part contains cartoons, toys, games, and so on. Teenagers section contains college, stationary, movie actors, bikes, video games, and so on. Youth section contains images related to job, bikes, electronic gadgets, and so on. Adult section contains images related to property, politics, news, and so on.
- *Gender dataset:* It mainly has two categories male and female. Male section contains vehicles, sports, gadgets, and other male related images. Female section contains images such as accessories, jewellery, television shows, and other female related images.
- *Profession dataset:* It contains images related to different professions such as engineer, doctor, lawyer, student, teacher, and many more.
- *Miscellaneous dataset:* In order to introduce randomness in the dataset, images related to abstract images, emojis, traffic signals, famous international figures, paintings, and several more are also included.

7.2 Probability of guessing password

During the login phase, user is required to select four pass images from the 25 pass images.

Case 1. For an illegitimate person to login, he/she must select four pass images from $^{25}C_4$ sets of images. This is for the case under the assumption invalid user has no idea about the actual user or his pass images set. In this case, the probability for guessing password is as follows.

$$P1 = 1/^{25}C_4 == 1/12650 == 0.00008,$$

where P1 = probability of guessing password in Case 1.

Case 2. This is the case under the assumption invalid user has knowledge about the valid user consecutive login sessions pass image set. However, the invalid user still has to choose password from the eight common images along with four pass images.

$$P2 = 1/^{12}C_4 == 1/495 == 0.0020,$$

where P2 = probability of guessing password in Case 2.

The probability P2 is also less. If the number of invalid login attempt sessions limit is crossed, then the login attempt is restricted for 5 hours. If the attacker again enters wrong password, then the valid user is intimated about this issue and is asked to change password. The probability for guessing password in Case 2 is slightly better than that of Case 1. However, it is not even close to .1. Moreover, proper strategy is applied to intimate the legitimate user regarding the necessary steps to be taken.

7.3 Prevents brute-force attacks

- **Case 1.** Generally, educated guess attacks are possible if the attacker has prior knowledge about the user. Distorting the images with a blur index minimizes this attack because the attacker cannot recognize the distorted version of the images. In addition, blur index is not constant, which means it changes for every successive login session. The proposed system also contains other approach to resist these educated guess attacks. In the registration phase, user should provide the information like age, profession, religion, country, gender. Based on this information, the image set of 5×5 -image grid is created that contains the images exactly

opposite to the taste of user. In this way, the proposed scheme can safeguard the educated guess attacks.

- *Case 2.* The attack implies successive trials of all the combinations of images until a valid password is obtained. In the proposed scheme, we are limiting the login attempts by restricting the user to login the system at most two times for a particular login session.

7.4 Prevents phishing attacks

Phishing attacks trick users into revealing their credentials by cloning legitimate websites. The user id that is provided during the time of registration will be converted to an image, which will be further divided into two shares—user share and server share using visual cryptography technique.

The user share is sent to user via email and the server share will be stored in the server's database. When the user logs in, he/she submits the user share and then the corresponding server share is retrieved from the database. A combined version of user share and server share shows the user id of the user. User can confirm the identity of website when the true id is displayed. This is possible because the original system only contains the server share and the fake website cannot have this as the server share image is hashed and stored in database.

If the user id is not appeared after combining both user share and server share, then user must request to change the share of the user as the previous one is with the attacker and the account can be compromised. The account now will be locked for few hours until a new share is communicated with the user. This way, the phishing attacks are prevented.

7.5 Prevents hidden camera attacks

Password capture attacks directly obtain passwords by intercepting user-entered data or tricking users into divulging passwords. As users enter login information, an attacker may gain knowledge about their credentials by external recording devices, such as video cameras. High-resolution cameras with telephoto lenses and surveillance equipment make a real concern if attackers target specific users and have access to their geographic location. Thus, the proposed scheme prevents hidden camera attacks by not highlighting the images selected by user during the login phase.

Some attacks involve password reconstruction instead of direct capture. For example, the attacker reconstructs user secrets in a few seconds by observing a few numbers of logins. The first login session contains 21 random images and 4 pass images

7.6 Prevents sniffing attacks

Simple network sniffing and wiretapping allow trivial capture of sensitive information, and this is possible on graphical authentication systems too. Sniffing attacks are possible when data are transmitted across public channels and/or unencrypted.

As we are blurring the images to resist educated guess attacks, the blur index of every image will be different for every login session. Therefore, the hash values of four pass images will be different. For instance, during the first login session, the attacker sniffs and stores the hash values of the images. During second login session, he/she again sniffs and compares the hash values of previous images with the current ones, and can try to guess the four pass images. Thus, if we use different blur index for every login attempt, the hash values changes. Even if he sniffs and compares, he/she cannot obtain pass images. However, the alteration of blur index should be within a feasible range in order to ensure user identification of the images. Hence, sniffing attacks cannot be possible on the proposed authentication scheme (Table 1).

7.7 Removal of similar pass images

Many of the too similar images were removed from the database. This has greatly contributed towards the high success of the system. The images used were downloaded from various sources from Internet. In total we had 1200 images for all categories. Of this we removed too similar images, which led to a total of 979. These images were removed because during development and testing we found that we ourselves were not able to distinguish between too similar images. Development team felt that this might lead to confusion which will affect usability and security of the system. Later actual users who were not able to either register or login indicated the similarity between the images as the key factor for their failure. This similarity may not be an issue for recall based system like username and password. For example password may contain capital I, small l, one 1 or pipe | as a character in password which are all confusing but still acceptable. This confusion may not be a problem with recall based system but it affects the usability of the recognition based system. Hence exclusion of such too similar images is a significant factor for success of image based systems.

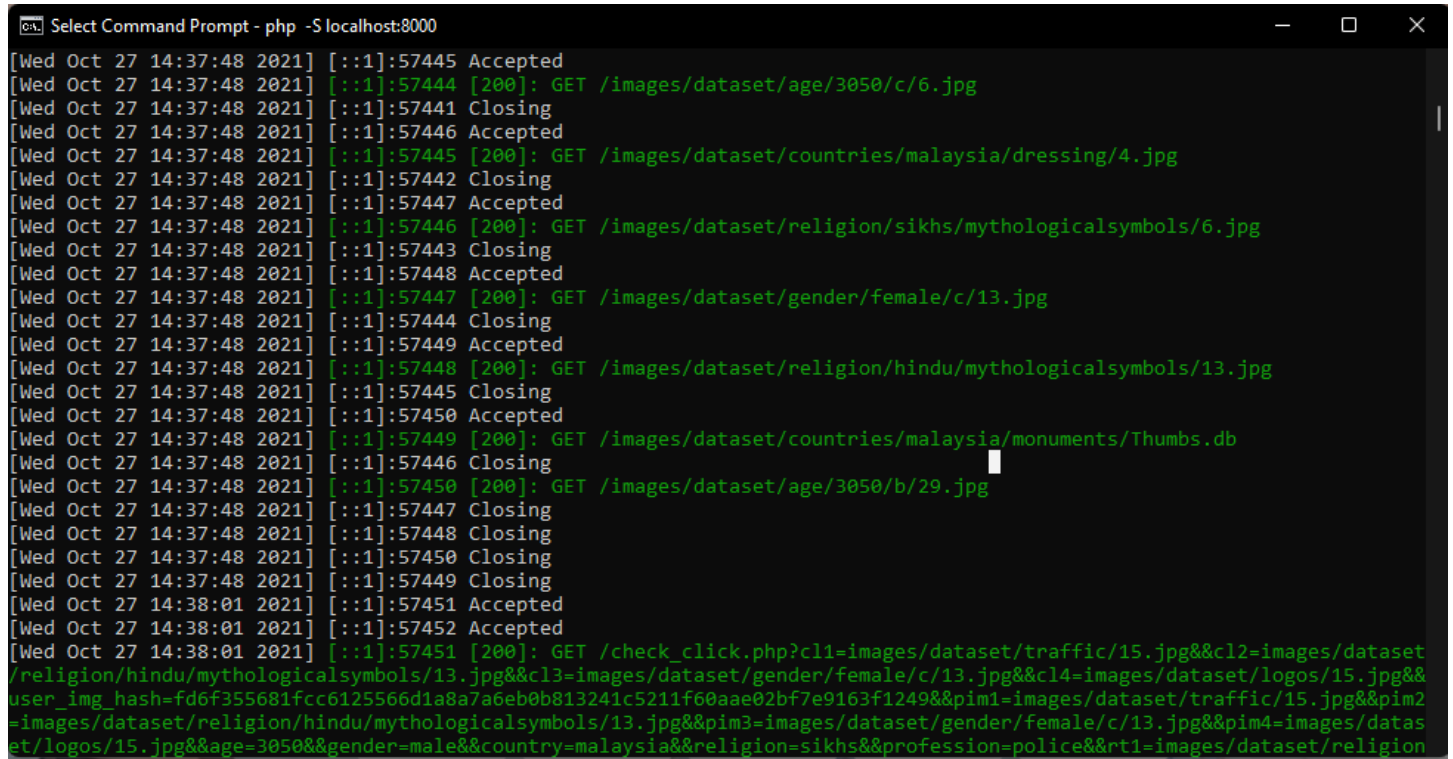
7.8 Evaluation of time consumption

We monitored the time required to register with the system and verification of images. We found that the time required to select pass images is less as compared to select new password. This might be because system assist user to select pass images. It is difficult to always come up with new secure password which is easy to memorize and recall. Verification time for the password was faster as compared to pass images. This was because that password verification requires only one round whereas our system requires multiple images to be verified. However user's survey indicates that the time for our system was reasonable.

7.9 Flexibility in selection of pass images

Traditional username password system support ASCII characters. However not all systems supports all 256 ASCII character set. Majority of the current system allows users to form password from typically 60 characters (upper case, lower case, numerals and some special characters). However in our system, user can select pass images from a set of 979 images. This gives user flexibility to select pass images which they can easily recognise later. While this is one of the key factors for the success of the system, it has negative consequence as well. It might be a time consuming task to browse through images. However users have indicated that it was a good experience to browse through images rather than to think of a new good password which is strong and easy to recall.

7.10 Screenshots



```
Select Command Prompt - php -S localhost:8000
[Wed Oct 27 14:37:48 2021] [::1]:57445 Accepted
[Wed Oct 27 14:37:48 2021] [::1]:57444 [200]: GET /images/dataset/age/3050/c/6.jpg
[Wed Oct 27 14:37:48 2021] [::1]:57441 Closing
[Wed Oct 27 14:37:48 2021] [::1]:57446 Accepted
[Wed Oct 27 14:37:48 2021] [::1]:57445 [200]: GET /images/dataset/countries/malaysia/dressing/4.jpg
[Wed Oct 27 14:37:48 2021] [::1]:57442 Closing
[Wed Oct 27 14:37:48 2021] [::1]:57447 Accepted
[Wed Oct 27 14:37:48 2021] [::1]:57446 [200]: GET /images/dataset/religion/sikhs/mythologicalsymbols/6.jpg
[Wed Oct 27 14:37:48 2021] [::1]:57443 Closing
[Wed Oct 27 14:37:48 2021] [::1]:57448 Accepted
[Wed Oct 27 14:37:48 2021] [::1]:57447 [200]: GET /images/dataset/gender/female/c/13.jpg
[Wed Oct 27 14:37:48 2021] [::1]:57444 Closing
[Wed Oct 27 14:37:48 2021] [::1]:57449 Accepted
[Wed Oct 27 14:37:48 2021] [::1]:57448 [200]: GET /images/dataset/religion/hindu/mythologicalsymbols/13.jpg
[Wed Oct 27 14:37:48 2021] [::1]:57445 Closing
[Wed Oct 27 14:37:48 2021] [::1]:57450 Accepted
[Wed Oct 27 14:37:48 2021] [::1]:57449 [200]: GET /images/dataset/countries/malaysia/monuments/Thumbs.db
[Wed Oct 27 14:37:48 2021] [::1]:57446 Closing
[Wed Oct 27 14:37:48 2021] [::1]:57450 [200]: GET /images/dataset/age/3050/b/29.jpg
[Wed Oct 27 14:37:48 2021] [::1]:57447 Closing
[Wed Oct 27 14:37:48 2021] [::1]:57448 Closing
[Wed Oct 27 14:37:48 2021] [::1]:57450 Closing
[Wed Oct 27 14:37:48 2021] [::1]:57449 Closing
[Wed Oct 27 14:38:01 2021] [::1]:57451 Accepted
[Wed Oct 27 14:38:01 2021] [::1]:57452 Accepted
[Wed Oct 27 14:38:01 2021] [::1]:57451 [200]: GET /check_click.php?c1=images/dataset/traffic/15.jpg&c12=images/dataset/religion/hindu/mythologicalsymbols/13.jpg&c13=images/dataset/gender/female/c/13.jpg&c14=images/dataset/logos/15.jpg&user_img_hash=fd6f355681fcc6125566d1a8a7a6eb0b813241c5211f60aae02bf7e9163f1249&pim1=images/dataset/traffic/15.jpg&pim2=images/dataset/religion/hindu/mythologicalsymbols/13.jpg&pim3=images/dataset/gender/female/c/13.jpg&pim4=images/dataset/logos/15.jpg&age=3050&gender=male&country=malaysia&religion=sikhs&profession=police&rt1=images/dataset/religion
```

Figure 15: Working of server

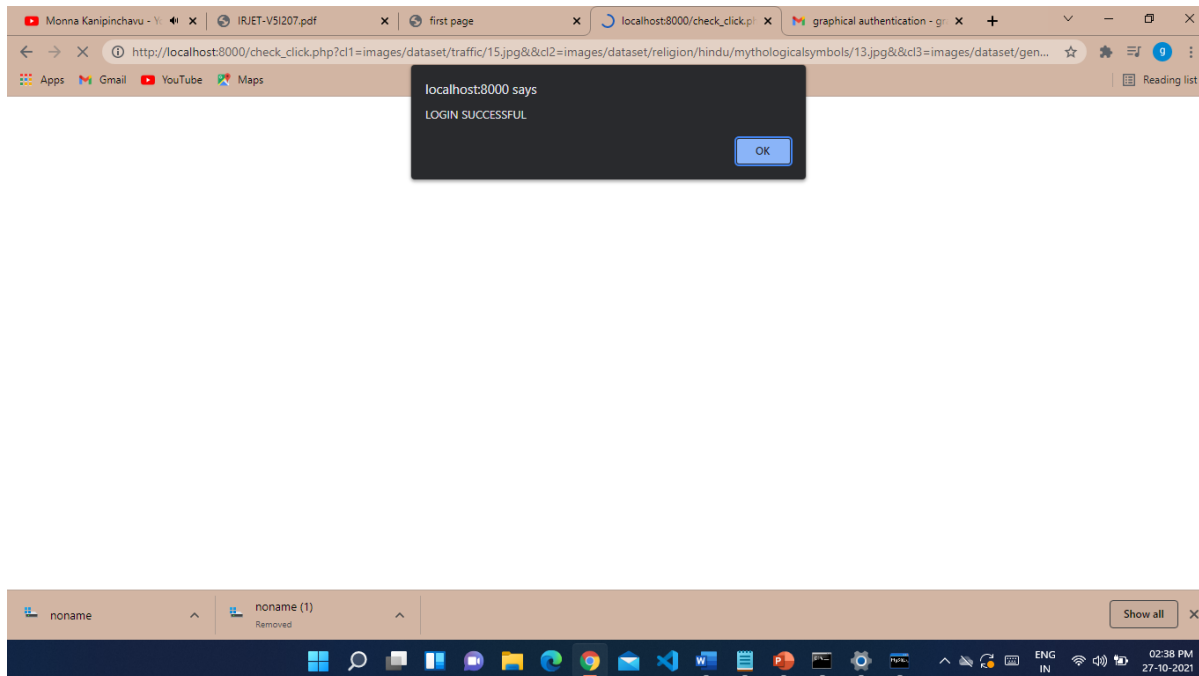


Figure 16: Login Successful.

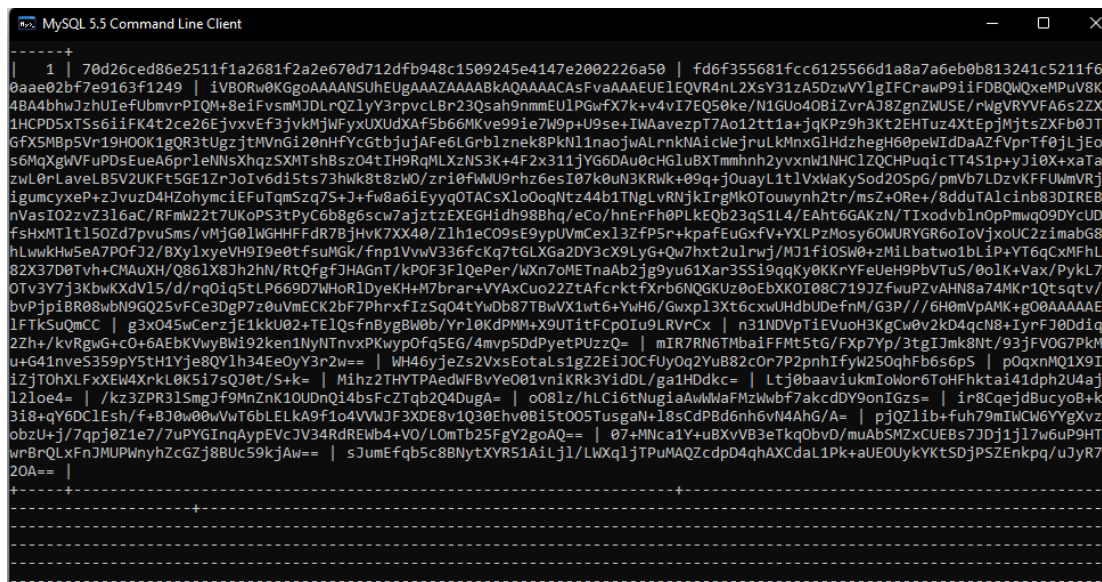


Figure 17: User data stored is encrypted and stored in Data Base.

TABLE 1. Comparison of security and performance attributes

Attributes	Awase-E	Passface	Proposed scheme
Prone to hidden camera attacks	Yes	Yes	No
Prone to shoulder surfing attacks	Yes	Yes	No
Prone to guessing attacks	Yes	No	No
Prone to phishing attacks	Yes	Yes	No
User-friendly	Yes	Yes	Yes
Easy to remember	Yes	No	Yes
Fast execution	No	Yes	Yes

ADVANTAGES:

- Fast execution
- User-friendly
- Probability of guessing password is low
- Prevents brute-force attacks. After three unsuccessful attempts user account gets locked. This can be unlocked by the administrators.
- Prevents phishing attacks
- Prevents hidden camera attacks
- Prevents sniffing attacks
- Add one more layer of security to the existing system and hence makes the system more secure.

- Login in by sharing of password is prevented as user needs to provide the pass images to login, sharing of pass images is difficult.
- Prevent automated attack by the bots.
- Eliminate the possibility of deducing the user's images set by means of an intersection attack.

LIMITATION OF THE SYSTEM:

- System cannot prevent offline dictionary attacks
- Slower than traditional username password system as loading of image grid takes some time.

8. CONCLUSION

The proposed graphical authentication scheme deployed some of the finest existing features such as distorted images, hash index, and loci metrics while introducing visual cryptographic techniques and additional naive features to defend the renowned attacks such as brute-force, educated guessing, sniffing, hidden camera, shoulder surfing, and phishing. The discussion section depicts that every feature in the proposed scheme resists one or more attacks. Literature study evident that majority existing authentication schemes experience a trade-off between security and performance. However, the proposed system has followed a layered architecture to induce better security that result in good performance. All the security related features are implemented in the background to enable any kind of user access the proposed scheme, which is marking it user-friendly. Furthermore, no special hardware or software is required to build this scheme that makes it simple.

High success rate indicates that authentication based on images can be used successfully for a particular purpose. A functional system was developed and user survey was carried out for seventy real users. Users were successfully able to recognize pass images from a group of images. It was not just based on the recognition but also on recall. This is because many users associated some images with some recall hints specifically for random images. For eg some random images appears to be a highway. However users favoured images with animals, objects rather than random art or abstract images. We implemented system along with username and password, but it can be implemented independently also.

9. BIBLIOGRAPHY

- Dhamija R, Perrig A. Deja Vu-A user study: using images for authentication. Paper presented at: USENIX Security Symposium, vol 9; 2000:4.
- Alavalapati GR, Yoo K-Y. Study of authentication techniques for next generations. Paper presented at: 2014 Summer Conference of Electronics Engineers in Korea; 2014:2135-2137.

WEBSITES:

www.w3school.com

www.w3school.com

www.w3school.com

www.google.com

REFERRED URLS:

<http://index.html>

<http://index.php>

<http://index.python>

<http://en.wikipedia.org/wiki/MYSQL>