GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Application Development Report Submitted
In partial fulfillment of the requirements for the award of the degree of

Bachelor of Technology
in
Electronics and Communication Engineering

by

J.AJAY KUMAR	**20N31A0491**
G.HEMA	**21N35A0408**
K.JYOTHI	**21N35A0411**

Under the esteemed guidance of

Mrs.T.MANASA VEENA
Asst. Professor

Department of Electronics and Communication Engineering

Malla Reddy College of Engineering & Technology
(Autonomous Institution- UGC, Govt. of India)
(Affiliated to JNTUH, Hyderabad, Approved by AICTE, NBA &NAAC with 'A' Grade) Maisammaguda, Kompally, Dhulapally, Secunderabad – 500100
website: www.mrcet.ac.in

Malla Reddy College of Engineering & Technology

(Autonomous Institution- UGC, Govt. of India)

(Affiliated to JNTUH, Hyderabad, Approved by AICTE, NBA &NAAC with 'A' Grade) Maisammaguda, Kompally, Dhulapally, Secunderabad – 500100 website: www.mrcet.ac.in

CERTIFICATE

This is to certify that this is the bonafide record of the mini project entitled **"Graphical Password Authentication System"**, submitted by **J.AJAYKUMAR (20N31A0491), G.HEMA (21N35A0408)** and **K.JYOTHI (21N35A0411)** of B.Tech in the partial fulfillment of the requirements for the degree of Bachelor of Technology in Electronics and Communication Engineering , Department of Electronics and Communication Engineering during the year 2021- 2022. The results embodied in this mini project report have not been submitted to any other university or institute for the award of any degree or diploma.

Internal Guide

Mrs.T.Manasa Veena
Asst.Profeesor

Head of the Department

Dr.K.MallikarjunaLingam
Professor & HOD

External Examiner

DECLARATION

We hereby declare that the mini project titled “Graphical Password Authentication System” submitted to Malla Reddy College of Engineering and Technology (UGC Autonomous), affiliated to Jawaharlal Nehru Technological University Hyderabad (JNTUH) for the award of the degree of Bachelor of Technology in, Electronics and Communication Engineering is a result of original research carried-out in this thesis. It is further declared that the mini project report or any part thereof has not been previously submitted to any University or Institute for the award of degree or diploma.

J.AJAYKUMAR - 20N31A0491

G.HEMA – 21N35A0408

K.JYOTHI- 21N35A0411

ACKNOWLEDGMENTS

We extend our gratitude to **Dr. VSK. Reddy, Director, Malla reddy college of engineering and technology, Hyderabad**, for facilitating us to present the Mini Project.

We wholeheartedly express our deep sense of gratitude to our beloved **Principal**, **Dr S. Srinivasa Rao**, for providing us adequate facilities for our successful completion of project work.

We extend our gratitude to **Prof P. Sanjeeva Reddy, Dean International Studies, Malla reddy college of engineering and technology, Hyderabad**, for facilitating us to present the Mini Project.

We would like to thank **Dr. K.Mallikarjuna Lingam, Head of the ECE Department**, for providing the freedom to use all the facilities available in the department, for successful completion of project.

We are grateful to our **Project Coordinator, Mr.Anup Dey , Asst. Professor**, for extending his support and cooperation throughout our project work.

We are very much thankful to our **Project guide Mrs.T.ManasaVeena, Asst. Professor**, for her extensive patience and guidance throughout our project work.

We would also like to thank all my **friends** for providing help and moral support at the right timing. With great affection and love, we thank our **parents** who were the backbone behind my deeds.

By

J.Ajaykumar (20N31A0491)
G.Hema (21N35A0408)
K.Jyothi(21N35A0411)

CONTENTS

Title	Page No.
Cover page	I
Certificate	II
Declaration	III
Acknowledgement	IV
Abstract	3
Chapter 1- Introduction	4-5
1.1 Background	4
1.2 Problem statement	4
1.3 Objectives	5
1.4 Applications	5
Chapter 2- Methodology	6-7
2.1 Block diagram	6
2.2 Description	6
2.3 Proposed method	7
Chapter 3- Flowchart & algorithm	8-10
3.1 Flowchart	8
3.2 User case diagram	9
Chapter 4-Software development	11-12
4.1 Introduction to Matlab	11
4.2 Testing/Experimentation	11
Chapter 5- Result	13-14
5.1 Input & output images	13
Chapter 6- Conclusion & Future scope	15
6.1 Conclusion	15
6.2 Future Scope	
Appendix: Source code	16-17
References	18

LIST OF FIGURES

TITLE OF FIGURE	PAGE NO.
Block Diagram	**6**
Flow chart	**8**
User case Diagram	**9**
Matlab Images	**12**
Input Image	**13**
Output Image	**14**

ABSTRACT

Computer security depends largely on passwords to authenticate human users from attackers. The most common computer authentication method is to use alphanumerical usernames & passwords. However, this method have significant drawbacks. For example, users tend to pick passwords that can be easily access. On the other hand, if a password is hard to access, then it is often hard to remember. Text-based password scheme follows the guidelines such as at least 8 characters long, should combine upper case and lower case and digits. User have problem to remember their complicated password over time due to limitation of human brains, user tend to forget about their passwords. User tends to use the same password for all types of accounts. So,if one account is hacked , the possibility for other account to be hack is high. Hence graphical password authentication system scheme has been introduce in this project. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this application, we conduct a comprehensive survey of the existing graphical password techniques. Graphical passwords provide a promising alternative to traditional alphanumeric passwords. They are attractive since people usually remember pictures better than words.

CHAPTER -1

INTRODUCTION

1.1 Background

Authentication is the process of determining that the person requesting a resource is the one who it claims to be. Most of the authentication system nowadays uses an integration of username and password. The problem with the password is that it requires user to remember it and it should be kept secret. Each authentication system has its own guidelines and limitations like password length, password must contain alphanumeric and special characters. These passwords are mostly text-based passwords. Either user use passwords that are easy to remember like license plate number, parent name, phone number sometimes their own name which are very much predictable or complex passwords which they overlook so they might be use the same password for different accounts or they jot down their password somewhere. Moreover, user is vulnerable to various attacks. Text-based passwords faces from security and usability matters.

To overcome these shortcomings of alphanumeric passwords, graphical password schemes have been proposed. In graphical password authentication application scheme a password contains an image where user can input password with the help of mouse events like click and drag. Picture Superiority Effect Theory reveals that pictures can be recognized and recalled easily by human brain, enhancing the ability to. Strong passwords can be invented which are resistant to guessing, dictionary attack and social engineering.

1.2 Problem Statement

The problem statement that can be describe in this project are user have problem to remember their complicated password over time due to the limitation of human brain, user tend to forget about their password. Next, user tent to use the same password for all type of account. So, if

one account is hacked, the possibility for other account to be hack is high. Therefore, choosing the simple textual passwords may increase its vulnerability for attacks or intrusions.

1.3 Objectives

The first objective of the research

i)To design a Graphical Password Authentication implemented in mobile application.

ii) To implement the Graphical Password Authentication application using PassPoint technique.

iii)To test the effectiveness of Graphical Password Authentication system using PassPoint technique to authenticate user by using web-based system.

1.4 Applications

1.Various Banking
2.Shopping websites
3.Email systems
4.Mobile Applications

CHAPTER-2

METHODOLOGY

2.1Block Diagram

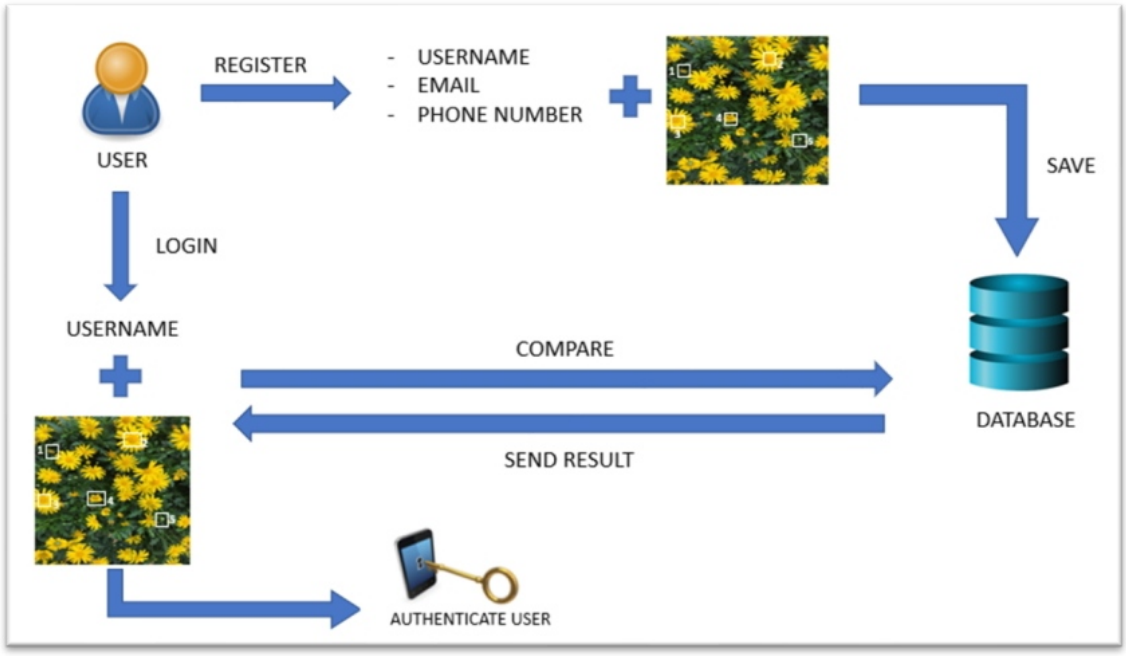


Fig.2.1- Block Diagram

2.2 Description

Block Diagram is a sketch of following process that allows how the system works and happen. Figure 2.1 shows that user can register to the system by enter username, email and phone number and then user is required to select a picture displayed. At this point, user need to click any five points in the picture that had been chosen before. After that, registration information will be saves in database. During login phase, user need to insert the username that has been registered during registration phase. Then, user is required to verify the picture displayed in the application that they had choose during registration phase.

After that, user is required to click five points that they clicked during the registration phase respectively. The system will make a comparison by checking the information with database.

The database server will send result whether user have registered or not to the user. Finally, user will be authenticated if the information entered and given by user are all correct.

2.3 Proposed method

The proposed authentication system works as follows. At the time of registration, a user creates a graphical password by first entering a picture he or she chooses. The user then chooses several point-of-interest (POI) regions in the picture. Each POI is described by a circle (center and radius). For every POI, the user types a word or phrase that would be associated with that POI. If the user does not type any text after selecting a POI, then that POI is associated with an empty string. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant.

For authentication, the user first enters his or her username. The system, then, displays the registered picture. The user, then, has to correctly pick the POIs and type the associated words. At any time, typed words are either shown as asterisks (*) or hidden. We believe that proposed approach is promising and unique for at least two reasons: It combines graphical and text-based passwords trying to achieve the best of both worlds. It provides multi-factor authentication (graphical, text, POI-order, POI-number) in a friendly intuitive system.

CHAPTER-3

FLOW CHART AND ALGORITHM

3.1Flowchart

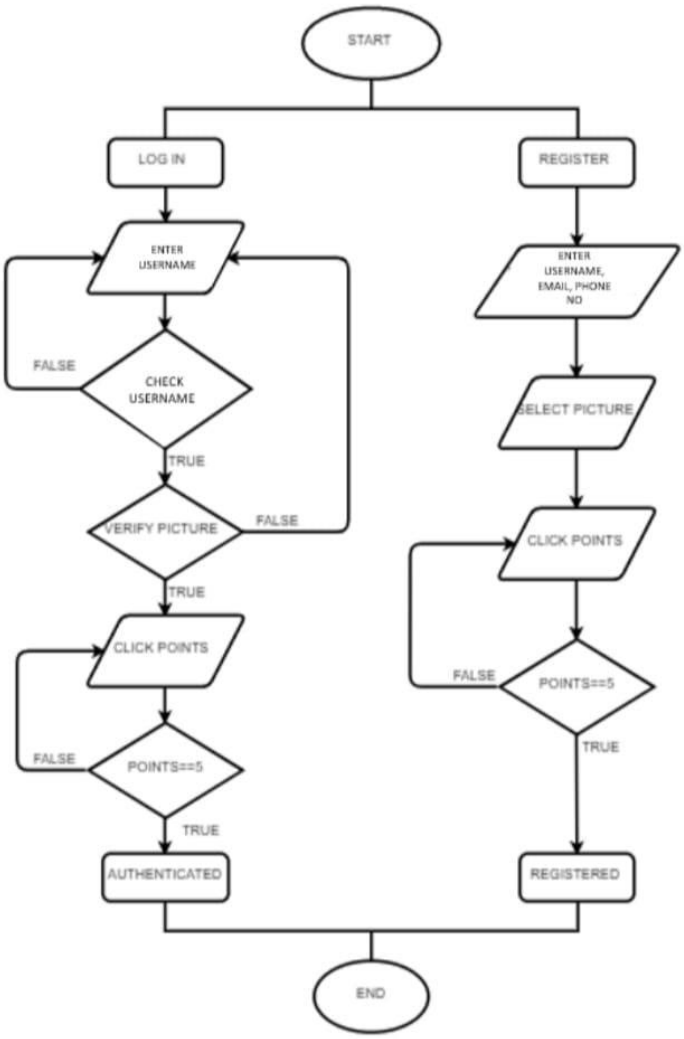


Fig 3.1-Flowchart

A flowchart is a diagram that describes a process, system or computer algorithm. In this section, the flowchart for implementing the project will be described. Figure 3.1shows the flowchart of Graphical Password Authentication. For registration phase, user will enter their names, email and phone number. After that, user is required to select a picture out of 30 images and then they will click five points within the image. User will legally registered after they had fill all of the requirements needed in the registration phase.

For log in phase, firstly user is required to enter their username that had been registered before. Then, there will be an image that user needed to verify either is it true that is their image or not. If it is, user need to click five spots that they had clicked during registration phase. Lastly, user is authenticated and they can log into the system.

3.2User case diagram

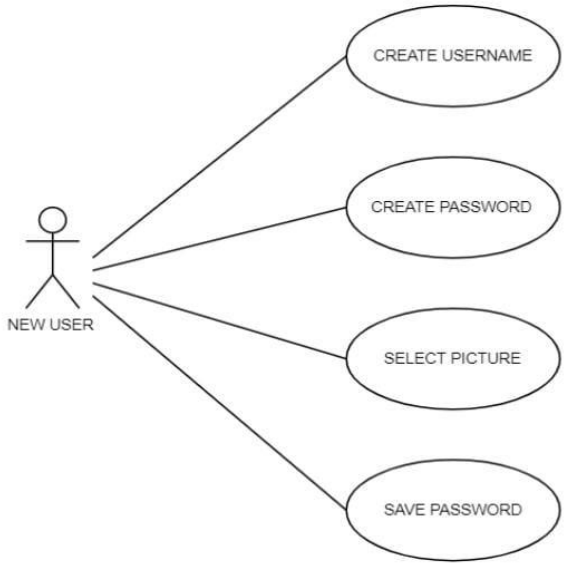


Fig 3.2.1:User case diagram for new user

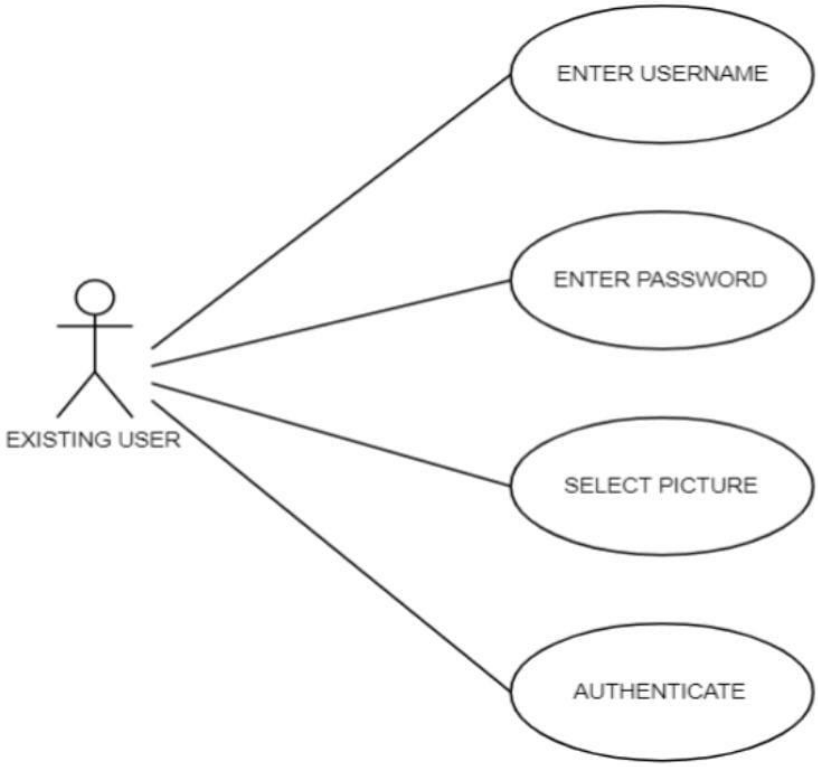


Fig 3.2.2 User case diagram for existing

Figure 3.2.1 shows the use case diagram for graphical password authentication using Passpoints scheme for new user. By looking at the diagram, four use cases will be found which are create username, create password, select picture and save password. Besides, the actor of this use case diagram is new user. Actor can be defined as something that interact with the system. The actor can be human user or internal and external application. Another important point is to identify the application boundary which are shown in the diagram. The actor user lies outside the system as it is an external user of the application.

Next, figure 3.2.2.show the use case diagram for graphical password authentication for existing user. There are also four use cases can be found in the diagram which are enter username, enter password, select picture and authenticate.

CHAPTER-4
SOFTWARE DEVELOPMENT

4.1Introduction to the matlab

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.
1.Typical uses include.
2.Math and computation.
3.Algorithm development.
4.Data acquisition.
5.Modeling, simulation, and prototyping.
6.Data analysis, exploration, and visualization.
7.Scientific and engineering graphics.
8.Application development, including graphical user interface building.

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar non interactive language such as C or FORTRAN. The name MATLAB stands for matrix laboratory. MATLAB was originally written to provide easy access to matrix software developed by the LINPACK and EISPACK projects. Today, MATLAB engines incorporate the LAPACK and BLAS libraries, embedding the state of the art in software for matrix computation. MATLAB has evolved over a period of years with input from many users.

4.2TESTING / EXPERIMENTATION

First, install MATLAB version 2014a or later on your system. Save the MATLAB source code file to graphical password a folder. Make sure the license plate image file is in the source code folder.

1. Run MATLAB from your desktop.
2. Open the graphical password file and click the Run menu button. You will be prompted to select an image file in .jpg format.
3. Select the image file that contains the license plate number. In this example, we used the p1.jpg file.

Continue to the next step. It shows the operation after executing the program. When the program is finished, enter the program and save it as a .m file in the Matlab folder. Then, when you run the code, a dialog box will pop up requesting the input image, which must be in JPG format. Select an image to open. Next, you will see an output image.

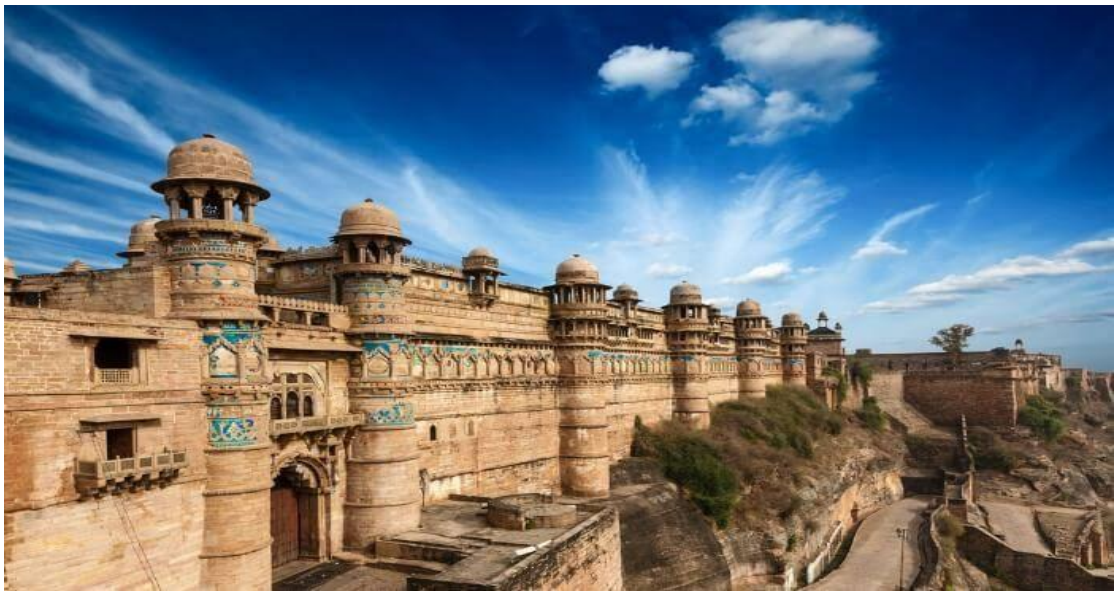


FIG 4.2.1

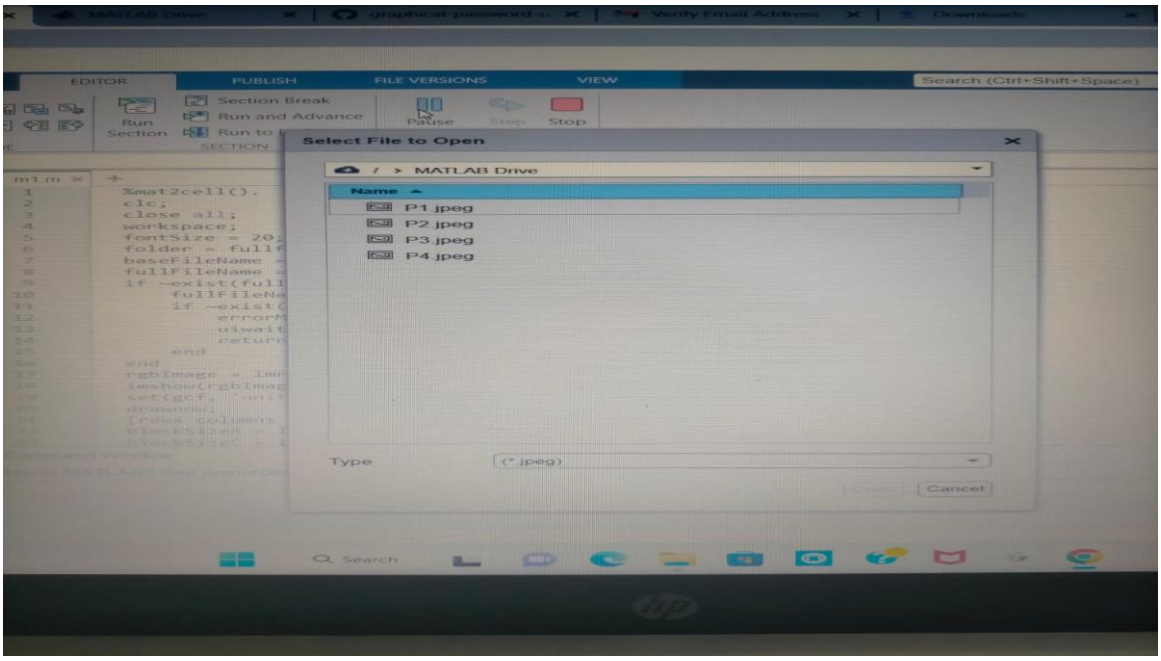


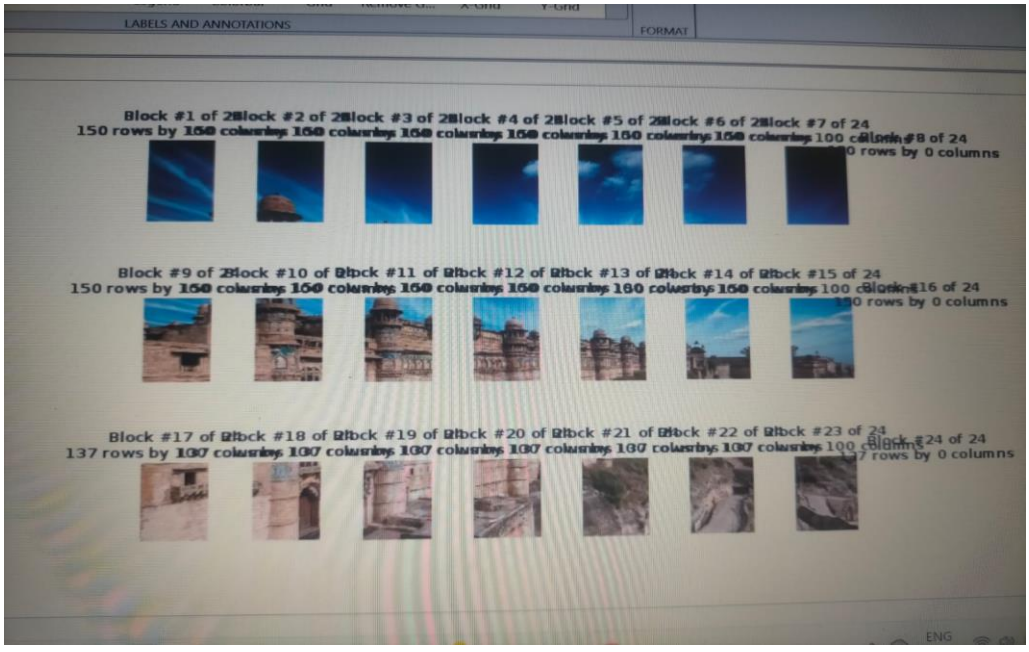
FIG 4.2.2-Matlab Images

CHAPTER-5

RESULTS

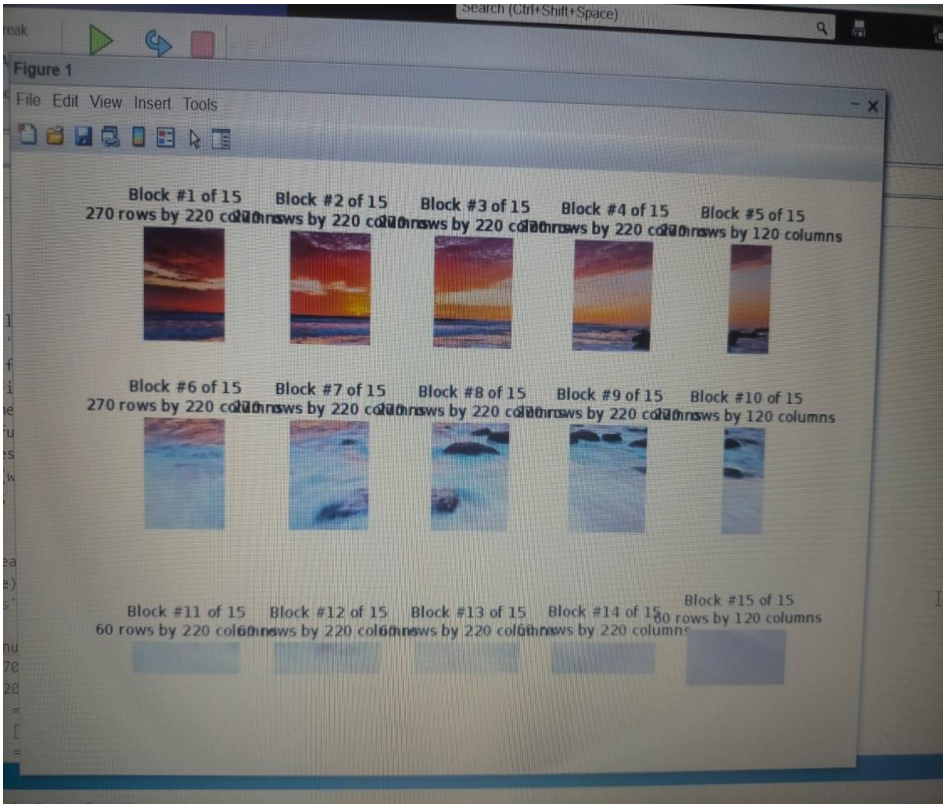
5.1 Input & output images

Fig (a)Input image



Fig(b)output image

Fig(c)-input image



Fig(d)-output image

CHAPTER 6

CONCLUSIONS & FUTURE SCOPE

6.1 Conclusion

User authentication is a fundamental component in most computer security context .In this extended abstract, we proposed a simple graphical password authentication system. The system combines graphical & text based passwords trying to achieve the best of the both worlds. It also provides multi factor authentication in a friendly intuitive system. As authentication techniques generate passwords but they have to face attacks like dictionary attacks, brute force attacks, shoulder surfing. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize.

6.2 Future scope

In the future, hopefully this system can be applied in real life because it may help users that have secret or privacy account want to keep their account private and protect their data privacy. To make this more secure the selection of every click points might be good if they have their own character or password. Researchers of modern days have gone through different alternative methods and concluded that graphical passwords are most preferable authentication system. By implementing encryption algorithms and hashing for storing and retrieving pictures and points, one can achieve more security. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess. Picture password is still immature more research is required in this field.

APPENDIX

SOURCE CODE

```
%mat2cell().
clc;
close all;
workspace;
fontSize = 20;
folder = fullfile(matlabroot, '\toolbox\images\imdemos');
baseFileName = 'peppers.png';
fullFileName = fullfile(folder, baseFileName);
if ~exist(fullFileName, 'file')
    fullFileName = baseFileName;
    if ~exist(fullFileName, 'file')
        errorMessage = sprintf('Error: %s does not exist.', fullFileName);
        uiwait(warndlg(errorMessage));
        return;
    end
end
rgbImage = imread(uigetfile('.jpeg'));
imshow(rgbImage);
set(gcf, 'units','normalized','outerposition',[0 0 1 1]);
drawnow;
[rows columns numberOfColorBands] = size(rgbImage)
blockSizeR = 270;
blockSizeC = 220;
wholeBlockRows = floor(rows / blockSizeR);
blockVectorR = [blockSizeR * ones(1, wholeBlockRows), rem(rows, blockSizeR)];
wholeBlockCols = floor(columns / blockSizeC);
blockVectorC = [blockSizeC * ones(1, wholeBlockCols), rem(columns, blockSizeC)];
if numberOfColorBands > 1
    ca = mat2cell(rgbImage, blockVectorR, blockVectorC, numberOfColorBands);
else
    ca = mat2cell(rgbImage, blockVectorR, blockVectorC);
end
```

```
plotIndex = 1;
numPlotsR = size(ca, 1);
numPlotsC = size(ca, 2);
for r = 1 : numPlotsR
   for c = 1 : numPlotsC
      fprintf('plotindex = %d,   c=%d, r=%d\n', plotIndex, c, r);
      subplot(numPlotsR, numPlotsC, plotIndex);
      rgbBlock = ca{r,c};
      imshow(rgbBlock);
      [rowsB columnsB numberOfColorBandsB] = size(rgbBlock);
      caption = sprintf('Block #%d of %d\n%d rows by %d columns', ...
         plotIndex, numPlotsR*numPlotsC, rowsB, columnsB);
      title(caption);
      drawnow;
      plotIndex = plotIndex + 1;
   end
end
```

REFERENCE

[1] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. p. 26.

[2] Aakansha Gokhale, & Vijaya Waghmare. (2013). Graphical Password Authentication Techniques: A Review. 7.

[3] Ahmet Emir Dirik, Nasir Memon, & Jean-Camille Birget. (2007). Modeling user choice in the PassPoints graphical password scheme. 8.

[4] Nelson, D. L., Reed, V. S., & Walling. J. R. (1976). Pictorial superiority effect. Journal of experimental psychology. Human learning and memory, 2(5), 523-528.

[5] Dhamija, R. (n.d.). Hash Visualization in User Authentication. 2. Khan, W. Z., & Aalsalem, M. Y. (19 December, 2013). A Graphical Password Based System for Small Mobile Devices. p. 11.

[6] Manjunath G. Satheesh K, Saranyadevi C, & Nithya M. (2014). Text-Based Shoulder Surfing Resistant Graphical Password Scheme. 4.

[7] Towseef Akram, Vakeel Ahmad, Israrul Haq, & Monisa Nazir. (2017).