User Authentication By Secured Graphical Password

(Result Paper)

Authors

Anil H.Rokade¹, Dr.Santosh S.Lomte², Prof.Rajesh A.Auti³, Yogesh R. Ngargoje⁴

Student, Department of Computer, Dr. SeemaQuadri Institute of Tech, Aurangabad, India¹
Professor, Department of Computer, Dr. SeemaQuadri Institute of Tech, Aurangabad, India²
Asst.Professor, Department of Computer, Dr. SeemaQuadri Institute of Tech, Aurangabad, India³
Student, Department of Computer, Dr. SeemaQuadri Institute of Tech, Aurangabad, India⁴
Email-Mr.anil2097@rediffmail.com, santoshlomte@hotmail.com, rajeshauti24@gmail.com
yogeshvcet1@gmail.com

ABSTRACT

Graphical passwords are considered to be a secure and memorable alternative to text passwords. Users of such systems, authenticate themselves by identifying a subset of images from the set of displayed images. However, despite the impressive results of user studies on experimental graphical passwords schemes, their overall commercial adaptations have been relatively low. In this paper, we investigate the reasons behind the low commercial acceptance of graphical passwords and present recommendations to overcome the same. Based on these recommendations, we design a simple graphical password scheme. It is aimed to work as a cued recognition based graphical authentication scheme that allows users to choose both text as well as images as their password with the same underlying design and interaction. In doing so, we blend the strengths of Numbers, Alphabets and Pictures together to effectively defeat prevalent forms of social hacking. We conducted a user study with 35 participants to evaluate the viability of our proposed design. Results of the study are encouraging which indicates that our proposed design is potentially secure.

Keywords :- User authentication, Graphical passwords, Security, high Probability, PIN.
INTRODUCTION

User authentication is a major problem in every system providing secure access to confidential information and personalized services. Although, today there exists numerous ways to authenticate a person [1][2], the most popular method amongst them is with passwords.

In this knowledge based authentication scheme, user authenticates his self by presenting the knowledge of a secret string of alphanumeric characters. The secret string is called as password and it is assumed to be known only to the claimed identity and hence her identity gets verified. However, in practice, anyone who knows or guesses the password is also able to authenticate as the legitimate user.

However, passwords are effective only if following two conflicting requirements are satisfied simultaneously.

Usability: Passwords should be easy to remember and user authentication process should easy for humans and should take less time.

Security: Passwords should be secure; that is, they should look random and should be hard to guess; they should be changed frequently and should be different on different accounts of the same user; they should not be written or stored down in plain text.

Unfortunately, most users find it difficult to come up with strong and secure passwords that they can easily recall without an external support. In effect, they typically choose simple dictionary words as passwords that are highly susceptible to guessing and theft [3][4][5]. On the other hand, if users are forced to use strong and random passwords, they write such passwords down or frequently forget them.

Either outcome defeats its intended purpose: that is to be secure and memorable at the same time. Ironically, attackers are experts in usability; they exploit these password malpractices by designing simple social engineering attacks to steal identity information [6].

These weaknesses in text passwords are now prompting for better authentication schemes that can balance the need to remember a password with the necessity of password being as random as possible.

A biometric based solution can solve the authentication problem in near future, if the cost of hardware comes down. Biometric solutions are fast, easy to deploy (with cheap hardware) and do not require remembrance. However, they are still very error prone at this stage and cannot be easily replaced once lost. Moreover, they can raise privacy concerns.

A better alternative to text passwords is graphical passwords. Graphical passwords are based on recall or recognition of visual information (Images, in particular) instead of alphanumeric strings. According to “Picture Superiority Effect” [7][8], humans have vast, almost limitless visual memory and images are remembered for a longer time, better than the text.
The success of the graphical password scheme strongly depends on the type of images used [9]. For example, user can create a portfolio using personal images or random images. Both approaches have advantages and disadvantages. Psychological results show that self-generated or personal images are better recognized than those that are not [10].

**1.3 Objectives**

The aim of this project is to investigate the reasons behind low commercial acceptance and provide suitable recommendations to overcome them. This project, based on these recommendations, we design a simple graphical password scheme, called user authentication by secured graphical password implementation.
User authentication by secured graphical password implementation is a cued recognition based graphical authentication scheme, which allows users to choose both text as well as images as passwords without any specific alterations to underlying authentication design and process.

**Theme**

User authentication by secured graphical password implementation is a novel cognometric graphical authentication scheme specially designed for keyless entry, which involves recognition of portfolio images.

### 2. RELATED WORK

The weaknesses of textual passwords became well known, researchers started exploring the feasibility of graphical passwords. It is widely known and verified by numerous psychological experiments that humans have superior visual memory and they can remember and recognize images for long time. Results show that recall of words declines by 50% or more over a 72 hour retention period compared with the recall of visual objects which drops only by less than 20% over the same period. In this section, we briefly catalogue the existing proposals on graphical passwords design. A detailed survey on graphical passwords schemes can be found in [1][2]. Existing approaches targeted towards exploring the power of pictures are mainly categorized in three categories: 1) Drawmetric Schemes 2) Locometric Schemes and 3) Cognometric Schemes.

**Drawmetric Schemes**

Drawmetric schemes are recall based authentication schemes, which require user to remember and repeat a visual drawing on predefined grid cells. Draw-A-Secret (DAS) [11] is one such scheme. In DAS, during enrolment, user creates a password consisting of an outline drawing of a figure on top of an image or a grid. To authenticate, she must recollect the drawing from her memory and redraw at the same place as before in the grid. However, the password space of such schemes is small as users prefer to draw symmetric images and with less number of strokes [12].

**Locometric Schemes**

Locometric schemes like Passpoints are based upon human skill to locate preselected points within an image. For example, in Passpoints scheme, the password is constructed with a series of random clicks on predefined regions of an image.

In order to login, user must repeat clicking on the same locations and in correct order. The PassPoints scheme design is shown in Figure 2.2.
However, recent studies have shown predictable patterns in user choices of click based password schemes. It has been observed that users choose distinct and semantically meaningful parts of an image as click points (called as hotspots), which reduce the overall password space, and hence the security of the proposed schemes is in doubt [13].

Chiasson et al. proposed an improvement over PassPoints, in the form of Cued Click Points (CCP) [6]. In CCP, user clicks on multiple images instead of clicking on multiple regions of single image. Although, CCP scheme increases attacker’s overload by increasing the number of images, it does not completely solve the problem of hot spots.

**Cognometric Schemes**

The graphical password schemes of our particular interest are Cognometric schemes. These schemes are based upon human ability to recognize previously learned pictures. Psychological research shows that humans are proficient in recognizing the Pictures they have seen before, even within a set of distracters.

**NAPTune Scheme**

NAPTune is a novel cognometric graphical authentication scheme which involves recognition of portfolio images. During account setup user creates a portfolio of 4 images or 4 characters or a 4-character word as her password and recognizes the images that corresponds to the chosen password to login. Motivation behind NAPTune came from Alphabet charts used in kindergarten schools to teach alphabets with the help of illustrative pictures (For example, A for Apple, B for ball etc). We adopt the same concept to develop a novel authentication scheme that can serve both alphanumeric and pictorial passwords with same underlying design and interaction.
3. SYSTEM DEVELOPMENT

Analytical Model

About Organization:

I know that what is aim of my Project so, according to that, I have collected all the necessary information, any type organization can use my project where security is more concerned (Example Banking Sector, Military, ATM, etc). For Handling of my project there is no age limit and also any level of educated person can use my project. My project is most efficient, easy to access and require low cost as compare to present system like biometry.

Analysis of Present System:

Text password

Text password security of password is the main issue now days. In text password cannot identify random password, it will not allow you to generate one time access code. Text password is weak against some of common attacks such as Brute force and dictionary based attack, Social engineering attack, Shoulder surfing attack, phishing attack, Malware attack.

Biometric password

A biometric password requires costly hardware. As it is related to biometric information it raises privacy concerns. In some cases it is seen that accuracy is not that much good. Today biometric password is very error prone.

Graphical Password

Security is important factor in every authentication schema. Graphical password provides highest security. The graphical password is providing more accuracy. Graphical password does not require any special hardware. So that cost of new hardware is saved.

Drawmetric Schemes

Drawmetric schemes are recall based authentication schemes, which require user to remember and repeat a visual drawing on predefined grid cells. Draw-A-Secret (DAS) is one such scheme.

In DAS, during enrolment, user creates a password consisting of an outline drawing of a figure on top of an image or a grid. To authenticate, he must recollect the drawing from his memory and redraw at the same place as before in the grid.

Drawbacks of Drawmetric schema

However, the password space of such schemes is small as users prefer to draw symmetric images and with less number of strokes.
Locometric Schemes-
Locometric schemes like Pass points are based upon human skill to locate preselected points within an image. For example, in Pass points scheme, the password is constructed with a series of random clicks on predefined regions of an image. In order to login, user must repeat clicking on the same locations and in correct order.

Drawbacks Locometric schemes
It has been observed that users choose distinct and semantically meaningful parts of an image as click points (called as hotspots), which reduce the overall password space, and hence the security of the proposed schemes is in doubt.
In small screen is very difficult to select particular point in image.

Cognometric Schemes
In Cognometric schemes, user typically memorizes a portfolio of images during enrollment and must distinguish those images from presented decoy images to login. These schemes are also viewed as Challenge-Response schemes, where the challenge is to correctly identify the images from the set of distracters.
The graphical password schemes of our particular interest are Cognometric schemes. These schemes are based upon human ability to recognize previously learned pictures. In this schemes images used is enter by user so security is doubtful.

Drawbacks Cognometric Schemes
However, research also shows that people remember images more accurately when they are semantically meaningful and generated by the people themselves. It makes design of Cognometric schemes even tougher, as self generated images are easy targets for an attacker to predict.

NAPTune Schemes
NAPTune contains only 5×5 grid. Which contains 25 image related to alphabet only. The password length is four. There are only 303600 possible patterns. In NAPTune ordering constraint is not kept. But also valid combination is reduces by 4!.

Drawbacks NAPTune Schemes
If ordering constraints is kept security is low. Due to this usability and security are low.

User Authentication by Secured Graphical Password Implementation Schemes-
User Authentication by Secured Graphical Password Implementation scheme provides more security as compare to above scheme by providing the 6×6 grid. This grid consist of both 26 letters in combination with 10 numbers(0 to 9) so that its possible combination get increased i.e1.4 x 10^9 (36P_4) or 1,402,410,240 possible patterns of selecting four images out of 36 images. Passwords generated by this scheme is secure;
that is, they generated randomly and it’s hard to guess, it changed frequently and it is different on different accounts of the same user. Our proposed scheme achieves the desired security without the aid of any extra hardware or token. It also does not need costly software installations or dedicated hardware to run. The login interface is intuitive and specially designed, keeping the cognitive abilities of the users in mind.

**Type of information require each activity**

There are two major activities in my project. One is registration activity and second is one login activity. For registration it requires 6*6 matrixes which include 26 character and 10 numbers. and 36 images. And for login it also require 6*6 matrix 36 images and each image contains the numbers only not characters.

**Information Processing Capabilities Require For Each System Activity**

In this I provides input in the form of characters, no’s, and images, using coding, processes the inputs and provide desire output. After that it will store all the information in data base and finally admin control all the things whatever he wants.

**3.1 System Architecture**

The Figure 3.1 shows the overall architecture of the system which shows the main components and modules for the development task.

**To Develop The Functional Requirement**

In this I provide the information to the end user or client how to use my application.

Steps during Registration-

Registration is one time event. During registration, we present user with a 6×6 grid consisting of 26 letters from the English alphabet set and 10 numbers employing count &write scheme (0 to 9) along with their pictorial representations as shown in Figure.
Registration step: User picks four images or characters and two numbers as password and enters the corresponding alphabet with number in the textbox shown below the image grid.

User is then free to choose any four images or four characters along with two numbers as her password. Irrespective of the selection (images or characters), he is allowed to enter only the four characters and two numbers in the textbox provided below.
To illustrate, even if user chooses images of Ice-Cream, Ball, Apple and Umbrella as his password along with two numbers- ONE and TWO. He must enter IBAU12 (The associated characters and numbers with those images) in the textbox. Once the user has submitted four characters and two numbers, a confirmation message is displayed about successful completion of registration.

Steps during Login-

During login, user sees the same 26 pictures and 10 numbers (0-9) randomly placed in the 6×6 image grid. However this time, the alphabets and numbers are replaced with a new set of numbers in the range of 0 to 9. In other words, each cell has a number instead of an alphabet associated with it as shown in Figure 1.4.

In order to enter, user needs to recognize password (six images as four password characters and two password numbers) and enter the associated number in the textbox below. Users who have chosen character and number as password should recall character and numbers, only then perform a visual search for images that correspond to the characters and numbers since the characters not visible on screen, instead a number is assigned to each image and the original set of numbers has been replaced with a new set of numbers during entry. The images here act as a cue for recalling the password.

![Figure 3.3 Login Windows](image)

**Figure 3.3 Login Windows**

Login Step: User recognizes the six password images and enters the corresponding numbers in the textbox shown below the image grid.

For example, for the password as IBAU12, user must locate the images of Ice-Cream, Ball, Apple, Umbrella, ONE, TWO in Figure 1.4; user must enter 266204 as password to login.

The numbers associated with the images keep changing with each login session and thus become the one time access code for a particular login session. Moreover, the numbers are repeated multiple times in the 6×6 image grid to thwart observation attacks.

Forget password-
If user forget his/her password then user has to click on Forget password link then it will ask you to enter that hint that you entered during registration after that it will send you password on that email id.

### 4. PERFORMANCE ANALYSIS

#### 4.1 Testing Process

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

#### 4.2 Result Analysis

**Text password**

In text password, security of password is the main issue now days. In text password cannot identify random password, it will not allow you to generate one time access code. Text password is weak against some of common attacks such as Brute force and dictionary based attack, Social engineering attack, Shoulder surfing attack, phishing attack, Malware attack. Accuracy is low in the text password. Cost of hardware is one of important factor but it does not require any special hardware. So cost of hardware is low.

**Biometric password**

A biometric password requires costly hardware. As it is related to biometric information it raises privacy concerns. In some cases it is seen that accuracy is not that much good. Today bio metric password is very error prone.

**Graphical Password**

Security is important factor in every authentication schema. Graphical password provides highest security. The graphical password is providing more accuracy. Graphical password does not require any special hardware. So that cost of new hardware is saved.
Drawmetric Schemes
Drawmetric schemes are recall based authentication schemes, which require user to remember and repeat a visual drawing on predefined grid cells. Security is low. Efficiency is also low. Usability is doubtful in Drawmetric schemes.

Locometric Schemes
Locometric schemes like Pass points are based upon human skill to locate preselected points within an image. In small screen is very difficult to select particular point in image. So that efficiency is very low as well as usability is also low.

Cognometric Schemes
The graphical password schemes of our particular interest are Cognometric schemes. These schemes are based upon human ability to recognize previously learned pictures. In this schemes images used is enter by user so security is doubtful. Efficacy is also low because to identifying correct image is hard. Due to that usability is low.

NAPTune Schemes
NAPTune contains only 5x5 grid. Which contains 25 image related to alphabet only. The password length is four. There are only 303600 possible patters. In NAPTune ordering constraint is not kept. But also valid combination is reduces by 4!. If ordering constraints is kept security is low. Due to this usability is low.

User Authentication by Secured Graphical Password Implementation Schemes-
User Authentication by Secured Graphical Password Implementation scheme provides more security as compare to above scheme by providing the 6×6 grid. This grid consist of both 26 letters in combination with 10 numbers (0 to 9) so that its possible combination get increased i.e. $1.4 \times 10^9$ ($36P_6$) or 1,402,410,240 possible patterns of selecting four images out of 36 images. Passwords generated by this scheme is secure; that is, they generated randomly and it’s hard to guess, it changed frequently and it is different on different accounts of the same user. Our proposed scheme achieves the desired security without the aid of any extra hardware or token. It also does not need costly software installations or dedicated hardware to run. The login interface is intuitive and specially designed, keeping the cognitive abilities of the users in mind.

User Study of User Authentication by Secured Graphical Password Implementation-

One aspect of my user study aimed to test the usability of user authentication by secured graphical password implementation. Is it simple? Is it easy to understand and convenient to use? Another goal of my user study was to learn the characteristics of user-chosen passwords in real system (i.e., in an environment where the passwords will be used frequently over a period of time).

Graph 4.2 Graphical passwords Schema
For example, do they contain dictionary words, do users prefer stories while creating passwords, what patterns they exhibit. In short, will they be easy to guess? If answers to most of these questions are affirmative then, my scheme can aid to memory benefits of earlier graphical authentication schemes.

Outline of the user study -

I integrated user authentication by secured graphical password implementation with a simple online course management portal. The access to the course content such as lecture notes, weekly exercise etc was protected with User authentication by secured graphical password implementation authentication scheme. The user study was conducted in the fall semester of 2013 in a second year computer Science Engineering university class, over a month’s period, from late November to late December. In total 35 subjects participated, including 32 undergraduate students, 2 graduate students (Teaching Assistants) and 1 professor. Twenty-five participants are male and 10 participants are female; the ages range from 20 to 45 with average of 22. The participants were from different regions of India, so apparently my participants represent a multicultural community.

At the start of the study, participants were given a 15-minute tutorial in the class by the first author of this paper. Because my user group consists of experienced computer users with solid computer knowledge and represents a relatively high education level, they might perform better than the general population in understanding my scheme.

To somewhat compensate for this, I only used plain language in the tutorial (no technical terms were mentioned, such as mapping of pictures to passwords or how a password is encoded). I estimate the attendance rate on the day of the tutorial was approximately 85%. My password scheme was then explained. Students were not given suggestions about how to choose a secure password or use any mnemonic strategy. A FAQ page was made available on the website in case they need help.

Procedure

Participants created the portfolio of password images from the set of presented images. The same set of thirty-six images was used for all the participants. Passwords were stored in the clear in the server to facilitate my access and study. As a part of training process, I requested the participants to try back-to-back login sessions in order to get familiar with the authentication process. For the remainder of the study, participants authenticate themselves at regular intervals to access the course content (i.e. to login to their accounts by recognizing their password images). At the end of the study, I requested participants to fill out questionnaires for the sake of qualitative analysis.
Table 4.3: Login Success rate and Mean time to login (in seconds)

<table>
<thead>
<tr>
<th>Time interval</th>
<th>Number of successful logins</th>
<th>Number of users with more than one login attempt</th>
<th>Mean time to login (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>After one day</td>
<td>97% (34/35)</td>
<td>4</td>
<td>29.5</td>
</tr>
<tr>
<td>After one week</td>
<td>86% (26/30)</td>
<td>11</td>
<td>23.7</td>
</tr>
<tr>
<td>After one month</td>
<td>77% (20/26)</td>
<td>14</td>
<td>27.1</td>
</tr>
</tbody>
</table>

RESULTS

I report the viability of user authentication by secured graphical password implementation in terms of: Accuracy (Number of successful Logins), Efficiency (Time required to login), Predictability (Password Strength) and User satisfaction.

Accuracy and Efficiency

I consider authentication to be successful, if the participant is able to login by correctly identifying her password images. Each participant was given a maximum of three attempts to login. If the user fails to login even after three attempts, then her password was reset on request.

I took three snapshots of the login process: after a day, after a week and finally after a month. Table 4.3 shows the combined results of Login Success rate and Mean time to login (in seconds) at the three respective snapshots. The numbers inside the parentheses are: (m / n) where m denotes number of successful participants while n denotes total number of participants.

Results show that, ninety four percent of the participants were able to login successfully in the first session. Five users needed more than one attempt to login to their respective accounts. After a week, I observed a dropout in terms of the login as only thirty out of the registered thirty five participants tried to login to user authentication by secured graphical password implementation. Twelve users made mistakes in login but six of them eventually succeeded (80% of participants were able to successfully login). In the final session of the user study which happened after one month, only 26 out of the 35 participants tried to login to user authentication by secured graphical password implementation. In this session, 18 out of the 26 participants were able to successfully login to their accounts with 15 participants required more than one attempt to login.
I admit that the long term memorability of the user authentication by secured graphical password implementation is relatively low in comparison with other schemes. However, I suggest that some simple modifications to the scheme would improve the memorability.

For example, 1) asking users to come up with a story, 2) using personal images instead of system selected images and 3) removing ambiguity between images (two users got confused between the images of guitar and violin while entering the password). These modifications are now part of my next round of studies.

Table also reports the details of the time required to login. As I can see, login times do not vary significantly across all the sessions.

The maximum delay occurred in the first session when participants were using the scheme for the first time and in the last session, which was after a month’s gap.

Although, the mean login time of more than 20 sec seems inappropriate for practical applications, I argue that following simple countermeasures can help in locating the password images faster in the login grid, thereby reducing the login time. For example, instead of randomizing the position of the images in the grid, if I keep them static (bound), it will help the users to locate their password images easily and in less time.

**Predictability**

With user authentication by secured graphical password implementation, I wanted to explore the common choices of passwords that users typically select. Since user authentication by secured graphical password implementation allows users to choose both picture as well as text, I were interested in finding the inclination of users (That is whether users will prefer text based user authentication by secured graphical password implementation passwords or image based user authentication by secured graphical password implementation passwords). These findings are important to determine the predictability of the passwords.

In the post study questionnaire, I asked the users to mention the type of password (text or image) they have used. Figure presents gender wise common patterns of the passwords collected from the participant’s responses.

During installation user creates a portfolio of 4 images or 4 characters or a 4-character word in combination with 2-numbers as her password and recognizes the images that corresponds to the chosen password to gain access into his home.

Motivation behind it came from Alphabet charts and numbers used in kindergarten schools to teach alphabets and counting with the help of illustrative pictures (For example, A for Apple, B for ball, ONE, TWO etc).

**Front End Design**

The Screenshot 4.1 shows three options which include following button

Tutorial: It just likes the manual for user. It contains description of steps for registration and login.
Tutorial is the guide line for user which helps user for creating account and shows general guide line. Tutorial is divided into two part information regarding registration and information regarding login.

In the registration part it gives information about every field and validation so that it help user. Registration: By clicking on this button user will get registration form. Where new user can register and create own account. It is one time process so that user has to create pass on one time during life cycle. If user have all ready created account then it will not all to create another account with same name. Login: By clicking on this button user will get Login form. Login is the process after registration it means user can only login when it is register successfully. If at the time of login user forget password then it may be recover by using e-mail id and hint which is provided at the time of registration.
Screenshot 4.2 shows registration form.
User has to fill up this form for doing registration. Here user has to enter first name it means initial name of user.

It must not be more than 20 char long. It must be character only.
The second field is last name it means surname of user it should not exceed limit of 20 characters.
User also has to enter date of birth by using calendar which is provided it has many way to enter date of birth such as by choosing number or by choosing month wise calendar.
At the last user fill email-id which must be valid so that user get conformation massage.
If user gives wrong password then it will not register successfully.
If user live empty field then message is shown to user.
Here you cannot use key board all entry must be by using virtual key board.
Right click event of mouse not working on this page.
After filling password user must click on continue button to move next step.
User can move previous step by clicking back button.
Screenshot 4.3 shows the registration form first step.
By clicking on continue button it will send verification code on entered email-id.
It will send six char verification codes.
It includes combination of character and number.
If user enter correct e-mail id then popup windows generated it shows message”Verification code send to e-mail please keep them handy to complete registration”.
If user enter wrong e-mail id then it will not send code.
If user not gets verification code it will not complete registration process.
Here you cannot use key board all entry must be by using virtual key board.
Right click event of mouse not working on this page.
After filling password user must click on continue button to move next step.
User can move previous step by clicking back button.
Screenshot 4.4 shows second step of registration.
Here user has to enter the verified code which is sending on entered email-id.
User also has to enter valid capuche.
User can also go back by clicking on back button.
By clicking on refresh capuche button string will be change.
It is very important step as it identify that user creating account is not fake user.
If it is fake user then it will not processed further.
Capuche identify that either it is human being or not.
It will also help to minimize load on server.
Right click event of mouse not working on this page.

After filling password user must click on continue button to move next step.

User can move previous step by clicking back button.

Screenshot 4.5 shows password screen which contain 26 characters images and 10 number (0 to 9) images.

All images placed randomly. It means every time place of each image is different.

Each image having character or number associated with it.

This window only shows when user in previous step enters correct information.

It is mandatory that password must contain four characters and two numbers.

![Screenshot 4.5 Registration Third Page](image)

It is mandatory that maximum length of password is six.

Here you cannot use key board all entry must be by using virtual key board.

Right click event of mouse not working on this page.

After filling password user must click on continue button to move next step.

User can move previous step by clicking back button.

User has to enter password which is combination of 4 character images and 2 numbers.

![Screenshot 4.6 Registration Fourth Page](image)
Screenshot 4.6 shows registration fourth step that is confirm password. Here user has to reenter password which is combination of 4 character images and 2 number images. The sequences of characters and numbers images are depending on user. He can give any sequence of these images but strictly follow this sequence during login. All images placed randomly. It means every time place of each image is different. Each image having character or number associated with it. This window only shows when user in previous step enters correct information. It is mandatory that password must contain four characters and two numbers. It is mandatory that maximum length of password is six. Here you cannot use keyboard all entry must be by using virtual key board. Right click event of mouse not working on this page. After filling password user must click on continue button to move next step. User can move previous step by clicking back button. User has to enter password which is combination of 4 character images and 2 numbers.

Screenshot 4.7 shows last step of registration. Here user has to enter the hint related to the password. This hint should give some information about password and it should describe the password. This hint is depending on user. If in future suppose user forget the password. These hints will help that user to remember the password. Hint must be meaningful so that it is remember for log time. Here you cannot use keyboard all entry must be by using virtual key board. Right click event of mouse not working on this page.
User can move previous step by clicking back button.
This is last step of registration after that user is register user.
By clicking on submit button user is register and message is display on screen.

Screenshot 4.8 Registration Successful Page

Screenshot 4.8 shows registration successful page.
Here user is successfully registered.
On the same page user can select three options.
From this page user can go at start page
By click on login page option it moves to login page.
New user can also start registration on same page.
After clicking on submit button of previous step if page display sign up successful message it means that user registration is successful.
It creates record in the database table.
Here you cannot use key board all entry must be by using virtual key board.
Right click event of mouse not working on this page.

Screenshot 4.9 Login Page
Screenshot 4.9 shows login window. Here user has to enter email-id which should be matched with registered email-id that enters at registration process.

After that user has to click on verify button then it will verify that email-id.

From this page user can go on start page

By click on sign up button user can move to registration page.

If user forget password then user has to click on ‘Forget Password’ link then it will show small window in that user has to enter hint that had entered during registration.

Here you cannot use key board all entry must be by using virtual key board.

Right click event of mouse not working on this page.

If user enter wrong email id then by click on reset button it will be reset.

![Screenshot 4.10 Login Second Page](image)

Screenshot 4.10 shows login second step.

Here user has to enter six digit number as password.

User has to enter numbers related to the images.

The image which is shown in registration same image is placed here.

The position of each image is change at every login.

At the same time new number is assign to each image.

Number must be in the range (0 to 9).

Each number is repeated maximum four times.

It can create one time password.

At next login the number enters by user is different one.
For example, for the password as IBAU12, user must locate the images of Ice-Cream, Ball, Apple, Umbrella, ONE, TWO in Figure 1.3; user must enter 266204 as password to login.

Here you cannot use keyboard all entry must be by using virtual key board.

Right click event of mouse not working on this page.

Password must match with previous password that enters at registration time.

![Screenshot 4.11 Login Third Page](image)

Screenshot 4.11 shows login page. Here user has to re-enter password.

Here user has to enter six digit number as password.

User has to enter numbers related to the images.

The image which is shown in registration same image is placed here.

The position of each image is change at every login.

At the same time new number is assign to each image.

Number must be in the range (0 to 9).

Each number is repeated maximum four times.

It can create one time password.

At next login the number enters by user is different one.

For example, for the password as IBAU12, user must locate the images of Ice-Cream, Ball, Apple, Umbrella, ONE, TWO in Figure 1.3; user must enter 266204 as password to login.

Here you cannot use keyboard all entry must be by using virtual keyboard.

Right click event of mouse not working on this page.

Password must match with previous password that enters at registration time.

Screenshot 4.12 shows home page.
This page will be displayed when user correctly re-enter password.
This window shows that user session will be start.
On this page user shows name which is enter at registration time.
Next field shows date of birth in YYYY-MM-DD format.

![Screenshot 4.12 Home Page](image1)

At third field e-mail shows e-mail address of user which is enter at registration time.
At the last user click here link option for logout.
Here you cannot use key board all entry must be by using virtual key board.
Right click event of mouse not working on this page.
Here user can only click on here link to logout.
So that user session is end.

Screenshot 4.13 Forget Password Page

Screenshot 4.13 shows forget password window
User must enter e-mail id which is register at registration process.
Here you cannot use key board all entry must be by using virtual key board.
Right click event of mouse not working on this page.

![Screenshot 4.13 Forget Password Page](image2)
5. CONCLUSION

Whenever we stored our data or any personal information anywhere that time security of our data is very important. So for that we have developed such system that has more security as compare to other system. This system generates secured Password; that is, they look random and it is hard to guess; they changed frequently and they are different on different accounts of the same user. They are not written or stored down in plain text. User Authentication by secure graphical password implementation is very secured system that protects our data from unauthorized use.

In this project, we have presented user authentication by secured graphical password implementation, a secure graphical authentication scheme, strong enough for banking, finance, e-commerce and sensitive organization. Its strength lies in its simplicity and unique graphical way of working. We have designed and secure prototype of user authentication by secured graphical password implementation. We discussed possible attacks on our scheme and how we could defend each of them. Results of the user study provide evidences for improved usability and memorability. Our future work includes working on the feedbacks received by the participants (using personal pictures and improving the visual search) and testing the scheme with large audience of all ages and under secure password inferences.

Future Scope

Graphical passwords are considered to be a secure and memorable alternative to text passwords.

We can use graphical password in net banking, mobile phones, Point of sale (POS) devices and ATMs, Keyless Entry, as it is more secure than the text password.

Passwords can be easily distributed, maintained and updated via telephone, fax or email and hence represent simple, cost effective and user friendly authentication solution.

Usability: Graphical Password is easy to remember and user authentication process is also easy for humans and takes less time.

Security: Graphical Passwords are secure; that is, they are hard to guess and look random; they are changing frequently and vary on different accounts of the same user; they are not written or stored down in plain text.

Graphical password scheme is aimed to work as a cued recognition based graphical authentication scheme that allows users to choose text and numbers in the form of images as their password for keyless entry into the home which increases the security and decreases the running cost of any other Keyless Entry Schemes (like Biometric systems such as finger print analysis, Iris recognition, etc)

5.3 Applications

In Banking Sector:
In bank for net banking graphical password is more secure than text password. So user authentication by secure graphical password implementation is more useful for net banking.

**In Smart Phone:**
Today in smart phone there are many password schemas but user authentication by secure graphical password implementation provides more security and it is more users friendly.

**ATM’s**
This schema is mostly developing for ATM’s where security is more important than any other thing. User authentication by secure graphical password implementation fulfills the need of user and more secure way to authenticate him.

**Keyless Entry**
User authentication by secure graphical password implementation is used in keyless entry at home and office. It can give more better way than previous key entry.

**Replace Biometric System**
It can also be use where biometric systems are used it can solve the problems that we can face in biometric system such as hardware failure.

**E-Commerce**
In most e-commerce application text password are used. As we know graphical password are more secure than text password. So we can replace text password with user authentication by secure graphical password implementation schema.

**ACKNOWLEDGEMENT**
It is my great pleasure in expressing sincere and deep gratitude towards my guide Dr. Santosh S. Lomte. I am also thankful to Head, Dept. of Computer Engineering, Prof. Rajesh A. Auti for providing me various resources and infrastructure facilities.
I also offer my most sincere thanks to Principal Prof. Venkatesh Gaddime, Everest College of Engineering, Aurangabad, my colleagues and staff members of computer science department, Everest college of Engineering, Aurangabad for cooperation provided by them in many ways.
I am very thanks to Prof. Zafar Ul Hasan for his valuable and firm suggestion, guidance and constant support throughout this work.
Last but not the list I am thankful to Miss. Shruti Sahare for her valuable suggestion. I would like to thank my friend Mr. Amit Mindhe for helping me in the making of this project. Finally I thanks to my all friends for their silent support and encouragement for this work could not have been possible.
REFERENCES