**Graphical Password Authentication Project Documentation**



Rahul Sharma

[rahultechip@gmail.com](mailto:rahultechip@gmail.com)

<https://github.com/mr-rahul-sharma>

<https://www.linkedin.com/in/rahul-2/>

**Index**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Topic** | **Page No.** |
| 1 | Introduction | 3 |
| 2 | Problem Definition | 5 |
| 3 | Objectives | 7 |
| 4 | Proposed System | 8 |
| 5 | Technical Details | 11 |
| 6 | Pros and Cons | 12 |
| 7 | Results | 13 |
| 8 | Discussion | 16 |
| 9 | Conclusion | 18 |
| 10 | References | 20 |

**Introduction**

Now a days people do not go to a bank to make a transaction, do not go to an Electric board to pay bill, do not go to railway station to make a train reservation and what not. All these times consuming and non-productive tasks are simplified because of Internet. To carry out these tasks everyone hits respective portals/sites or make use of a smartphone app. There are many such areas where we need human interaction with computers and these systems should be secured against Cybercrimes. User authentication is the most fundamental component in all computer security systems.

Security practitioners and researchers have made their efforts to protect systems and correspondingly, individual users’ digital assets. Because of increasing threats over the internet or networked computer systems, there is great need for preventions of such activities.

We use alphanumerical usernames and passwords for authentication purpose but studies shows that user can only remember a limited number of passwords. They tend to note them down somewhere or will use the same passwords for different accounts. In some cases, to avoid the complexity, users often pick passwords that is simple and easy to remember.

Biometrics is one of the various alternatives to increase the security but it requires lot of investments. To increase security to next level, some researchers have developed authentication methods that use pictures as passwords or a second level of authentication.

With increasing technical advancements, the world is becoming digital at a high pace and everything is happening online. From paying your bills to ticket bookings to paying the person sitting next to you, you prefer to pay online. Not only payments but all activities, be it, communication through e-mails and messaging apps, keeping your documents in a digital locker, etc happen online.

With everything turning online, the risk of cybercrimes and privacy breaches is also increasing. Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts. There are various types of authentications available for users to secure their accounts.

**Problem Definition**

Users have difficulty remembering complex, random passwords over time for their long-term memory limitation. A user is likely to forget a password that is not used regularly as the memory is not “refreshed” or “activated” sufficiently. Having multiple passwords, the user may either jumble the elements of the different passwords or confuse them of which system it corresponds to.

Users normally deal with the password memory problems by decreasing the complexity and number of passwords, which reduces password security. A secure password should be 8 characters or longer, random, with upper-case characters, lowercase characters, digits, and special characters. Users ignore such password recommendations, using instead short, simple passwords that are relatively easy to discover using dictionary attacks.

Recent surveys have shown that users often choose, short, alphabetic-only passwords consisting of personal names of family or friends, pets, etc. Users typically write down their passwords, sometime share the passwords with others, or use the same password for multiple systems.

Passwords are ubiquitous today on any platform, on possibly any website. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a project illustrating graphical password strategy. This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login o the system.

Considering the traditional username-password authentication, the alphanumeric passwords are either easy to guess or difficult to remember. Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them. Alternative authentication methods, such as biometrics, graphical passwords are used to overcome these problems associated with the traditional username-password authentication technique.

In order to Satisfy the shortcomings of the existing text-based Password Systems and to make the systems more secure from hacking and predictability we are developing a new generation of passwords that are based on images that cannot be easily predicted or hacked.

**Objectives**

In this method, the user is required to select some images (let’s say different chocolates) in a specific pattern (for example dairy milk is followed by 5 stars which is in turn followed by KitKat and so on).

Next time the user tries to log in, the images would have been shuffled, but the user will be required to follow the same pattern which was used initially.

Every time the user will have to use the same sequence while the images are placed in different ways.

This type of authentication is difficult to break since neither brute force nor dictionary attacks could breach it.

We need techniques that can be easily implemented and provide better results to this process.

**Proposed System**

Graphical passwords were first introduced by BLONDER in 1996. A graphical password is an authentication system which allows the users to select from images, in a specific order, presented in a graphical user interface (GUI). Graphical passwords can be easily remembered, as users remember images better than words.

In a graphical password authentication system, the user has to select from images, in a specific order, presented to them in a graphical user interface (GUI). According to a study, the human brain has a greater capability of remembering what they see(pictures) rather than alphanumeric characters. Therefore, graphical passwords overcome the disadvantage of alphanumeric passwords.

Graphical Password Authentication has three major categories based on the activity they use for authentication of the password:

Recognition based authentication

Recall based authentication

Cued Recall

**Recognition Based System:**

A user is given a set of images and he has to identify the image he selected during registration.

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

In recognition-based techniques, Authentication is done by challenging the user to identify image or images that the user had selected during the registration stage. Another name for recognition-based systems is search metric systems. It is generally required that users memorize a number of images during password creation, and then to log in, must identify their images among them. Humans have unique ability to identify images previously seen, even those which has been viewed very briefly. Recognition based systems have been proposed using usability and security considerations, and offers usability. In some graphical password schemes, Knowledge of some details of the shared secret must be retained by the system, i.e., user specific profile data e.g., in recognition schemes, the system must know which images belong to a user’s portfolio in order to display them.

Sobrado and Birget Scheme is recognition-based system that displays a number of pass-objects (pre-selected by user) among many other objects, user click inside the convex hull bounded by pass-objects. In Pass face scheme human faces are used as password. And in Dhamija and Perrig Scheme Pick several pictures out of many choices, identify them later in authentication.

**Recall Based System:**

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

In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Recall-based graphical password systems are occasionally referred as draw metric systems since a secret drawing is recalled and reproduced by the user. In these systems, users typically draw their password either on a blank canvas or on a grid. You can secure your password using various techniques in graphical authentication.

To authenticate, we use a grid-based approach by using image as a reference. Draw-A-Secret (DAS) Scheme User draws a simple picture on a 2D grid, the coordinates of the grids occupied by the picture are stored in the order of drawing. Redrawing has to touch the same grids in the same sequence in authentication. Then certain grids are selected by the user to set his/her password as shown in the figure below a major drawback of graphical password authentication is shoulder surfing.

Another one is Pass Point Scheme which allows users to click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, user must click within the tolerances in the correct sequence. Signature scheme is another graphical user authentication conducted by having the user drawing their signature using a mouse.

**Cued Recall:**

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

**Technical Details**

The developed project is a web application.

Here are some technical details about the project.

|  |  |
| --- | --- |
| Programming Language | Python |
| Web Framework | Django |
| Database | SQLite |
| User Model | Django default User model |
| Web Languages | HTML, CSS, JavaScript |
| Project Location | <https://github.com/mr-rahul-sharma/picpassword> |
| Project Website | <https://picpassword.herokuapp.com> |

Project location and project website may be unavailable.

**Pros and Cons**

*Advantages of graphical authentication method:*

The security of the system is very high.

Graphical password schemes provide a way of making more human-friendly passwords.

Dictionary attacks and brute force search are infeasible.

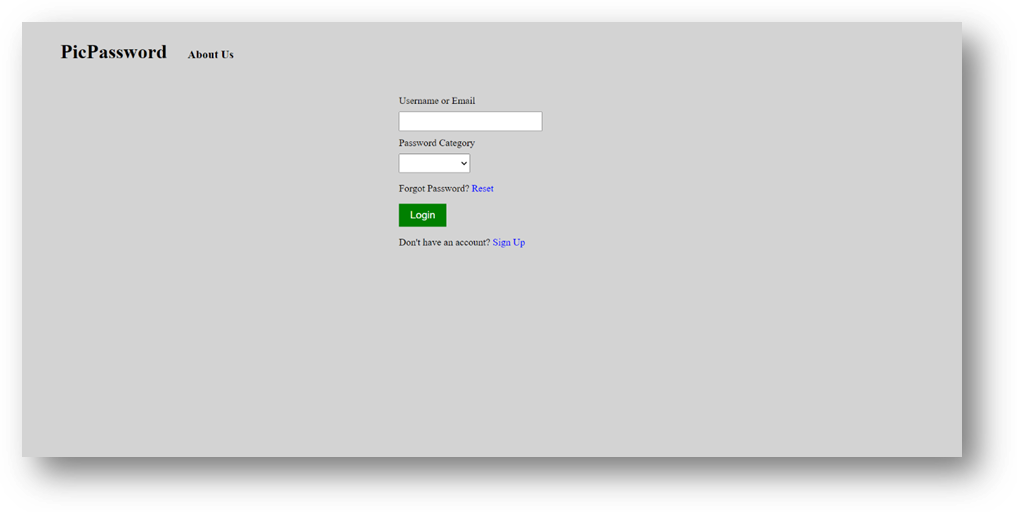
*Disadvantages of graphical authentication method:*

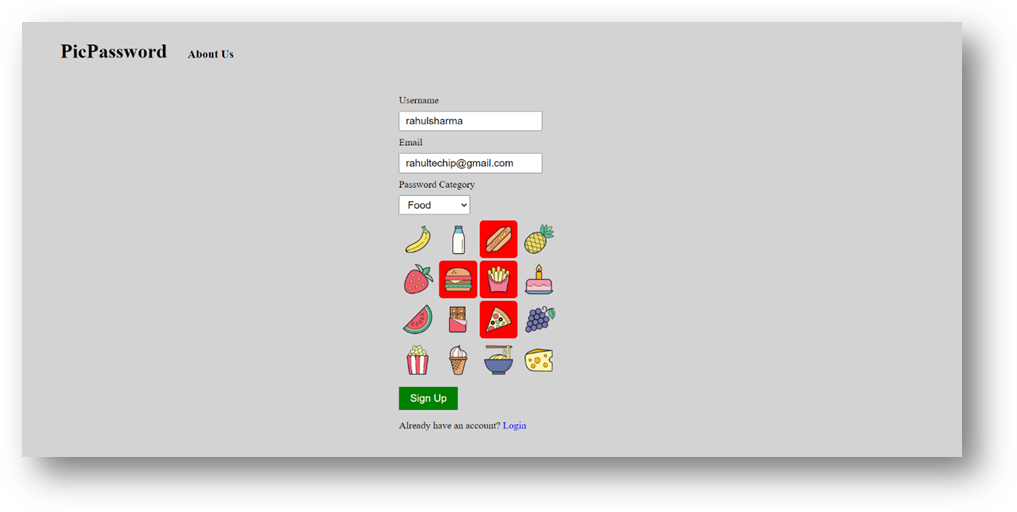
Require much more storage space than text-based passwords.

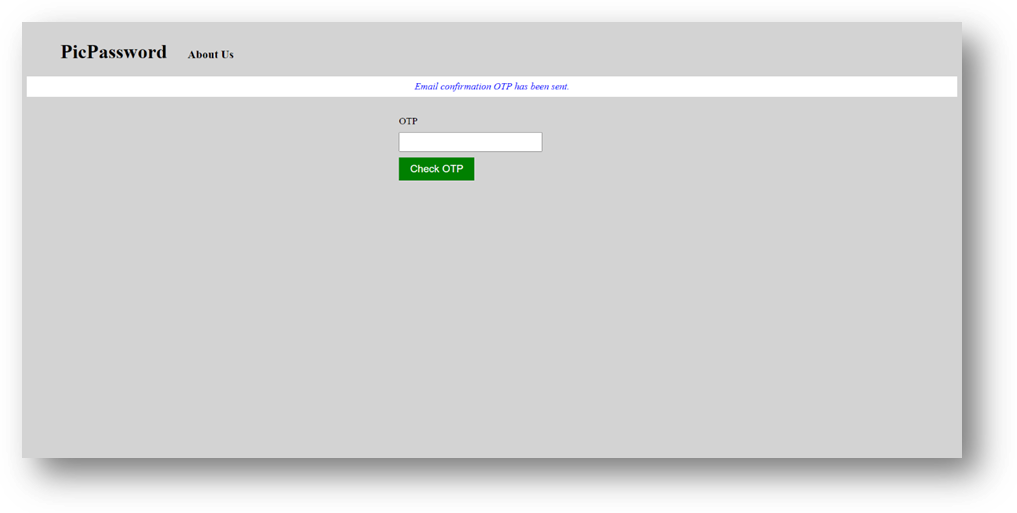
Password registration and log-in process take too long.

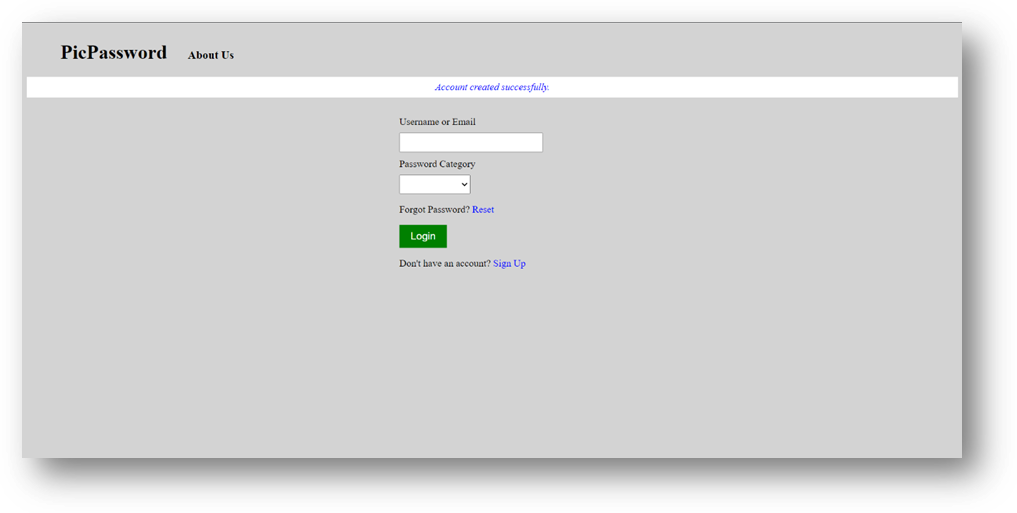
Shoulder Surfing: As the name implies, shoulder surfing is watching over people’s shoulders as they process information. Because of their graphic nature, nearly all graphical password schemes are quite vulnerable to shoulder surfing.

**Results**

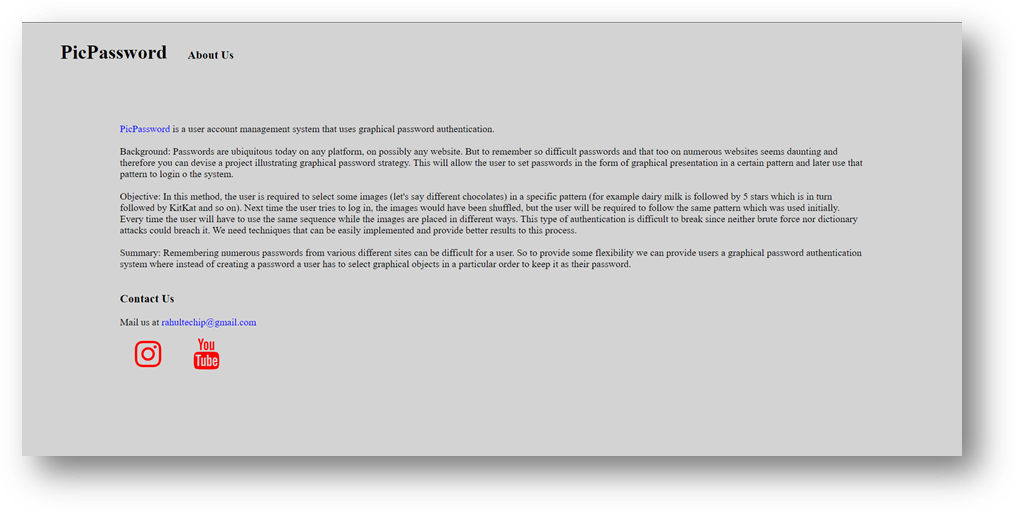












**Discussion**

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

Brute force search:

The main defense against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of Printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have smaller password spaces than the recall-based methods.

It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password.

Dictionary attacks:

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall-based graphical passwords it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text-based dictionary attack. More research is needed in this area. Overall, we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

**Guessing:**

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passface technique have shown that people often choose weak and predictable graphical passwords. Nali and Thorpe’s study revealed similar predictability among the graphical passwords created with the DAS technique. More research efforts are needed to understand the nature of graphical passwords created by real world users.

**Shoulder surfing:**

Like text-based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing. None of the recall-based based techniques are considered should-surfing resistant.

**Conclusion**

Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies support such assumption. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

Graphical passwords provide a promising alternative to traditional alphanumeric passwords. They are attractive since people usually remember pictures better than words. Remembering numerous passwords from various different sites can be difficult for a user. So, to provide some flexibility we can provide users a graphical password authentication system where instead of creating a password a user has to select graphical objects in a particular order to keep it as their password.

In general, graphical passwords techniques are classi-

ﬁed into two main categories: recognition-based and recall-

based graphical techniques [7]. In recognition-based tech-

niques, a user is authenticated by challenging him/her to

identify one or more images he or she chooses during the

registration stage. In recall-based techniques, a user is asked

to reproduce something that he or she created or selected

earlier during the registration stage

In general, graphical passwords techniques are classi-

ﬁed into two main categories: recognition-based and recall-

based graphical techniques [7]. In recognition-based tech-

niques, a user is authenticated by challenging him/her to

identify one or more images he or she chooses during the

registration stage. In recall-based techniques, a user is asked

to reproduce something that he or she created or selected

earlier during the registration stage

In general, graphical passwords techniques are classi-

ﬁed into two main categories: recognition-based and recall-

based graphical techniques [7]. In recognition-based tech-

niques, a user is authenticated by challenging him/her to

identify one or more images he or she chooses during the

registration stage. In recall-based techniques, a user is asked

to reproduce something that he or she created or selected

earlier during the registration stage

In general, graphical passwords techniques are classi-

ﬁed into two main categories: recognition-based and recall-

based graphical techniques [7]. In recognition-based tech-

niques, a user is authenticated by challenging him/her to

identify one or more images he or she chooses during the

registration stage. In recall-based techniques, a user is asked

to reproduce something that he or she created or selected

earlier during the registration stage

In general, graphical passwords techniques are classiﬁed into two main categories: recognition-based and recall-based graphical techniques. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, we have conducted a comprehensive survey of existing graphical password techniques. The current graphical password techniques can be classified into two categories: recognition-based and recall-based techniques.

Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood.

Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness.

**References**

Graphical Password: Wikipedia

<https://en.wikipedia.org/wiki/Graphical_password>

Graphical Password Authentication: GeeksforGeeks

<https://www.geeksforgeeks.org/graphical-password-authentication/>

Python Documentation

<https://docs.python.org/3/>

Django Documentation

<https://docs.djangoproject.com/en/4.0/>