IMG Secure – A Graphical Password Authentication System

Rishank Pratik
19BCE1606
Vellore Institute of
Technology, Chennai

Wilson Vidyut Doloy
19BCE1603
Vellore Institute of
Technology, Chennai

Prakrit Raj
19BCE1865
Vellore Institute of
Technology, Chennai

Abstract —***User authentication is an important way to ensure the security of your cyber account. Although there are various authentication methods such as iris and fingerprint, passwords will be the main authentication method for the time being due to their low cost and ease of implementation. But this ease of implementation is also a factor which makes it less secure compared to other methods. We have tried to design a system, based on images and grids and to develop a new system with the same ease of implementation but with more security with respect to common attacks. We have incorporated the principles used in captcha and pass point methods and developed a new system altogether which is developed as a module and can be integrated with any existing portal or system.***

Keywords— ***Graphical Password, Grid Mapping, Authentication, Image grid, Security*.**

I. INTRODUCTION

In today’s digital world, privacy is treated as a myth as there are various agents present all over the world who on finding a small crack in the system to steal information or compromise the system. Passwords are a primary measure to prevent unauthorized access to the system but as time passes on, these agents or hackers develop ways to find loopholes in the systems and bypass the basic security provided by it. Password cracking is the process of retrieving passwords from a computer or data transmitted by a computer. This need not be a sophisticated procedure. Password cracking is a brute-force assault that checks all potential combinations. If the password is stored in plaintext, a hacker can access all account information by hacking the database. Most passwords, however, are now saved with a key derivation function. This creates a 'hash' by running a password through a one-way cypher. The hash of the password is stored in the server.

Passwords provide the first line of defence against unauthorized access to any computer or security system. The stronger is the password, the more protected/secured a system will be from hackers and malicious software. Although there are many alternatives to passwords for access control, passwords are the most convincing credentials in many applications. They provide a simple and straight forward way to protect a system, and they represent an individual's identity and authentication to a system.

The main weakness of text-based passwords is their nature. Many times, these days, strong passwords are essential to protect personal data, as there are many ways for unauthorized people with little technical knowledge or skills to learn passwords for legitimate users.

Graphical Passwords when proposed in 1996, were aimed to provide an alternative to text-based passwords by providing an easy to remember [1]-[4] as found in various studies of human brain and provide more security with respect to text-based passwords against most common attacks such as brute-force attacks, shoulder surfing and keylogging spywares.

Our project is aimed at developing a Graphical password authentication system which is as easy it is to remember as difficult it is to crack. The structure of our paper is organised as follows. In section 2, we go through various other proposed works for a graphical or image-based password authentication system and analyse the methodology they have used. In section 3 & 4, We propose our own version of such authentication system and explain about the workflow of the architecture that we have worked upon and implemented. We would also discuss the various features we have implemented in the module and how they improve the security of the overall module. In section 5, we would do a comparative analysis of our developed system with various other existing image-based password authentication systems. In section 6, we offer the concluded summary and analysis of our work with the addition of future scope for this project.

II. LITERATURE SURVEY

We while going through past papers and patents where they various shortcomings of text-based password authentication systems. We found out that there are many approaches for a graphical password authentication system which proposed various different methods such as Image APIs, Captcha, Pass Points and many more. These proposed methods have been implemented in real-time but only as secondary authentication methods as they only prevent bot attacks. [6] discusses how Graphical passwords process authentication by selecting the exact positions on the image shown on the screen. A scheme called Captcha based authentication protocol is used alongside Pass Positions method. Captcha offers a novel approach to tackle the well-known image hotspot problem in popular graphical password systems. This scheme is resistant to usability issues such that it does not overload human memory and provides extra security against unwanted attacks. [7] focuses on the security aspects of existing graphical password schemes where they categorize existing graphical password schemes into four kinds according to the authentication style and review the known attack methods, categorize them into various kinds, and present some user studies of those schemes.

III. SYSTEM ARCHITECHTURE

Over the years, many processes or schemes which focus on different approaches to propose or implement a graphical password authentication system. These schemes are categorized as drawmetric schemes which focus on the memory capabilities of the user, locimetric schemes which focus on the focus points of a given image as in Pass Points method where different points or sectors are identified as valid and are required to be selected in order to proceed further, cognometric schemes which make use of an user's cognitive abilities to perceive something and try to relate it with their memory and hybrid schemes which use combinations of various different proposals under different categories to combine them and develop a new approach where the individual approaches try to reduce the collective risk and increase overall security with better metrics.

The architecture or workflow which we have developed for this given use case of authenticating users comprises of various different processes which work in unison to achieve the requirements of the system as shown in Fig 1. This system that we are proposing primarily uses the locimetric principles of Pass Points approach[6][7], hybrid principles of Captcha[6][7] approach with minor influence from other approaches[8][9].

As shown in the figure *x*, the architecture that we have proposed is of a hybrid one where the authentication process includes an image grid of minimum 4×4 dimension which can be modified or increased further. This grid retrieves the images and vectors from the secure database and displays them after distributing them randomly over the grid. After receiving the sequence from the user, it converts the data into a hash value and stores it with user details if not registered. In case, the user is registered, the same hash value is verified with the existing data present for authentication of the user. After which the user is redirected to the home page the module is attached to. But it restricts the access to the given account after a number of failed login attempts and blocks the account which can be retrieved only via the user details already present in the database for reauthentication of the user and changing the password.

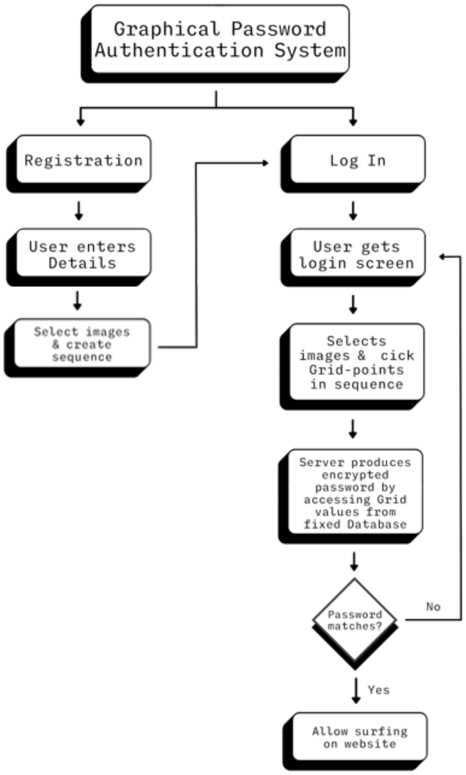

Graphical Password Authentication System
Registration
User enters Details
Select images & create sequence
Log In
User gets login screen
Selects images & cick Grid-points in sequence
Server produces encrypted password by accessing Grid values from fixed Database
Password matches?
No
Yes
Allow surfing on website

Figure 1: Architectural Flow Diagram

IV. PROPOSED METHODOLOGY

The system we propose includes certain concepts from captcha and pass points and tries to combine them in a new approach to address various security concerns related to the login modules. It takes the concept of pass points to form a grid of images which are not necessarily part of one image and are fragments of multiple images or vectors shuffled.

The very first requirement is the storage of images in a database from where they can be retrieved for authentication purposes by the web application. This database holds the various different images and vectors which are to be used for user authentication.

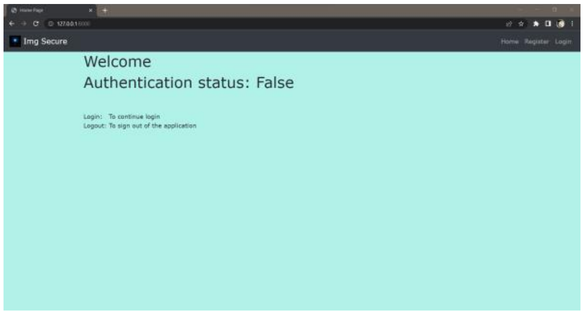
Next comes the securing of user information of various users who have registered with the web application. This information majorly includes the Basic user details and the password information which here is the sequence of images. This is implemented using sets where a password set is created for each user to store the image grid sequence in the database.

This set of image grid points sequence is received from the user when trying to log in to the system to be compare with the existing records to verify the authenticity of the user.

V. IMPLEMENTATION

In order to successfully demonstrate the use of our proposed architecture and methodology, we implemented this concept with the help of Flask, HTML, CSS and Python scripts.

With the use of python commands, the web application is loaded onto the browser.

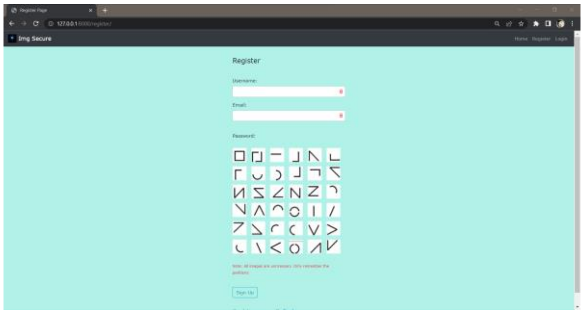


Welcome
Authentication status: False

Login: To continue login
Logout: To sign out of the application

Figure 2: Home Page

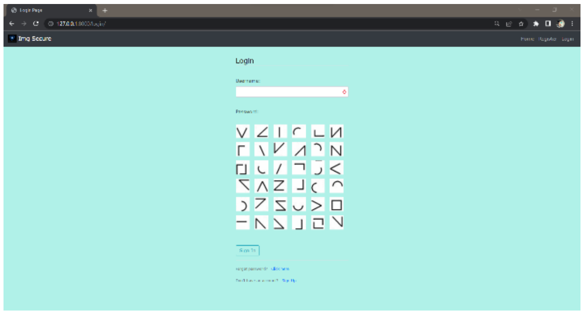
The homepage initially shows the current authentication status with the menu options to register or login to the system as shown in Fig 2.



Note: All images are unnecessary. Only remember the positions.

Figure 3: Registration Page

The registration page requires the user to enter their credentials such as user name and email address. After that the user is required to select the image grid sequence they want to keep as their password. It is also notified to the user that the images themselves have no importance as passwords but the grid sequence matters as shown in Fig 3.



Forgot password? Click here
Don't have an account? Sign Up

Figure 4: Login Page

After successful registration the user is allowed to login to the system using their credentials and also reset their password sequence at the login page.

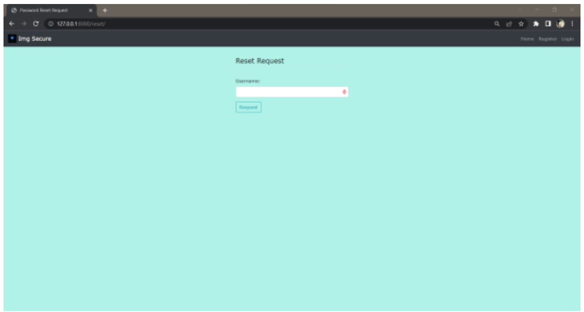


Figure 5: Password Reset Page

When requesting to change the password sequence the user is required to enter their username which would be verified with the existing records and the OTP to reset the password is shared with the user's email id registered in the database.

VI. RESULTS AND DISCUSSION

IMG Secure uses an image grid for authentication of the users where they have to select certain image boxes in a predetermined sequence with a minimum of 4 selections. Considering these facts, there are a various number of attacks which can be used by attackers to compromise the system which are discussed with reference to Table 2 & 3 and Fig 5 & 6.

A. BRUTE FORCE ATTACKS

These types of attacks continuously keep the system busy by trying to forcefully break in to the system with the use of iterations through all the possible combinations to guess the password. The equation to determine the number of possible password combinations for a n×n image grid with selection of minimum k=4 selections and their arrangements which can involve the complete image grid would be

$$\sum_{k=4}^{n^2} P_k^{n^2}$$

In our implementation, we have used a 6x6 image grid when implemented in the formula becomes

$$\sum_{k=4}^{36} P_k^{36}$$

and gives a value of $1.0111827005 \times 10^{42}$ which is very large compared to other existing possible combinations available for other existing authentication methods. This provides security against a variety of brute force attacks. Furthermore the number of possible combinations rapidly increases when using a larger grid as shown in Table 1.

n value	Possible Password combinations
4	$5.6874039550 \times 10^{13}$
5	$4.2163840398 \times 10^{25}$
6	$1.0111827005 \times 10^{42}$
7	$1.6534815375 \times 10^{65}$
8	$3.4491444202 \times 10^{90}$
9	$1.5758222319 \times 10^{123}$

Table 1 - Possible grid and password combinations

In addition to that, there is also a failsafe procedure, which locks the account after a number of failed login attempts to apply more complexity to the system and enhance the security against such attacks.

B. DICTIONARY ATTACKS

These types of attacks use a predefined set of combinations of values which may have been obtained from the personal information of the or may be completely random. Since IMG Secure uses an image grid to authenticate the users without the images having any impact on the authentication process. Even though the images used at the time of registration can affect the password sequence chosen, but the images always permute in the grid from the database. Thus the occurrence of the same grid which was at the time of selecting the passwords.

C. SHOULDER SURFING ATTACKS

These types of attacks employ the use of Spywares or individual agents who basically keep track of our login attempts while trying to get the authentication related information such as user name and image sequence.

To prevent this from happening, IMG Secure employs a technique which essentially hides the information regarding the image grids such as removing the highlight on the grid while toggling/selecting the image and hides any changes in the appearance of the user interface while logging in to the system. This removes the possibility of Shoulder surfing to obtain the passwords/image sequence while logging into the system.

D. KEYLOGGER ATTACKS

These types of attacks employ the use of malicious input devices such as an infected keyboard which may contain a spyware whose purpose is to send the keystroke information to the attacker who can retrace the steps to obtain confidential information.

Since there is no use of the keyboard for entering the passwords or the image sequence, it restricts most part of the attack on the system and prevents the passwords from being exposed.

E. SESSION ATTACKS

These types of attacks make use of session hijacking tools to obtain active session cookies and cookies related to logging information which are generally stored in browsers' cache memory as cookies.

IMG secure uses the image sequence to authenticate the users which is stored in the form of sets in the database where the elements are the grid boxes the user has selected. This information is impossible to store in form of cookies in the browser as they are designed to store alphanumeric passwords and prevents this types of attacks.

F. COMPARITIVE ANALYSIS

IMG Secure which is proposed to be a combination of both Locimetric & Cognometric Schemes, there are a various number of other methodologies which also exist derived out of these. These include Pass points, Cued-Click points, Pass Faces, Photographic authentication, Story, Awase-E, Déjà vu, Use Your Illusion, Colorlogin, Blonder and visKey.

The comparison between the different already existing Image or Graphical password systems with IMG Secure with respect to both cognometric and locimetric schemes is done in the Tables 2 & 3 with respect to vulnerability to different types of attacking methods discussed in Section 6. Also the comparative analysis of the password space of these various schemes and their comparison is also presented along with that of IMG Secure in the form of bar graphs in Fig 6 & 7.

Schemes	Password space (bit)	Dictionary Attacks	Tricking	Phishing or Pharming
Blonder	Unknown	Y	Middle	Middle
Pass Points	43	N	Difficult	Middle
visKey	Unknown	N	Difficult	Middle
CCP	43	N	Difficult	Difficult
PCCP	43	Y	Difficult	Difficult
IMG Secure	49	N	Difficult	Difficult

Table 2: Locimetric Schemes

Schemes	Password space (bit)	Dictionary Attack	Shoulder Surfing	Tricking	Phishing or Pharming	Spyware Attack
Déjà vu	16	Y	N	Difficult	Middle	Screen
PassFaces	13	N	N	Difficult	Middle	Screen
Photographic authentication	20	Y	N	Difficult	Middle	Screen
Awase-E	Unknown	Y	N	Difficult	Middle	Screen
Story	12	Y	N	Middle	Middle	Screen
Picture Password	Unknown	Y	N	Difficult	Middle	Screen
VIP	13	Y	Y	Difficult	Middle	Screen
Use Your Illusion	11	Y	N	Difficult	Middle	Screen
Colorlogin	Unknown	Y	Y	Difficult	Difficult	Y
GPI/GPIS	43	Y	N	Difficult	Middle	Screen
IMG Secure	49	N	N	Difficult	Difficult	Screen

Table 3: Cognometric Schemes

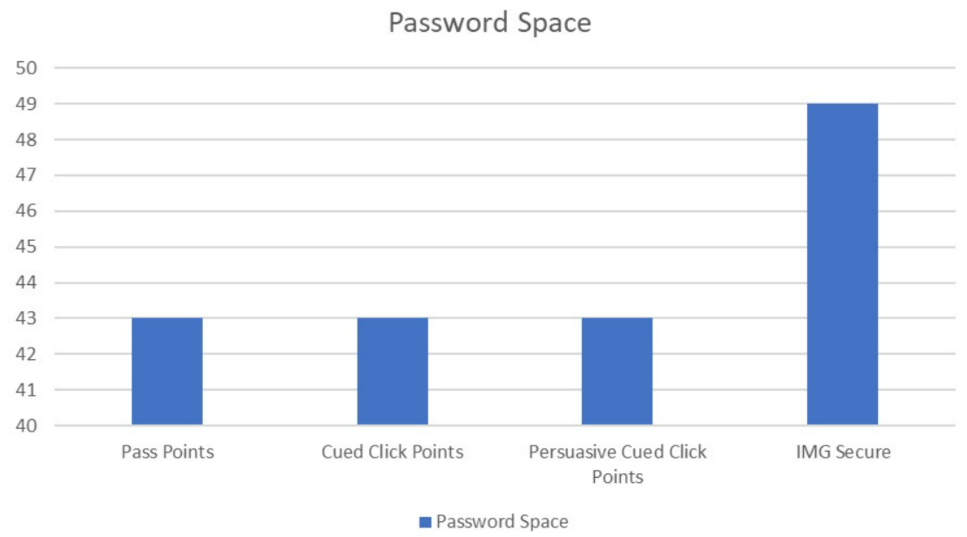


Figure 6: Password Space of Locimetric Schemes

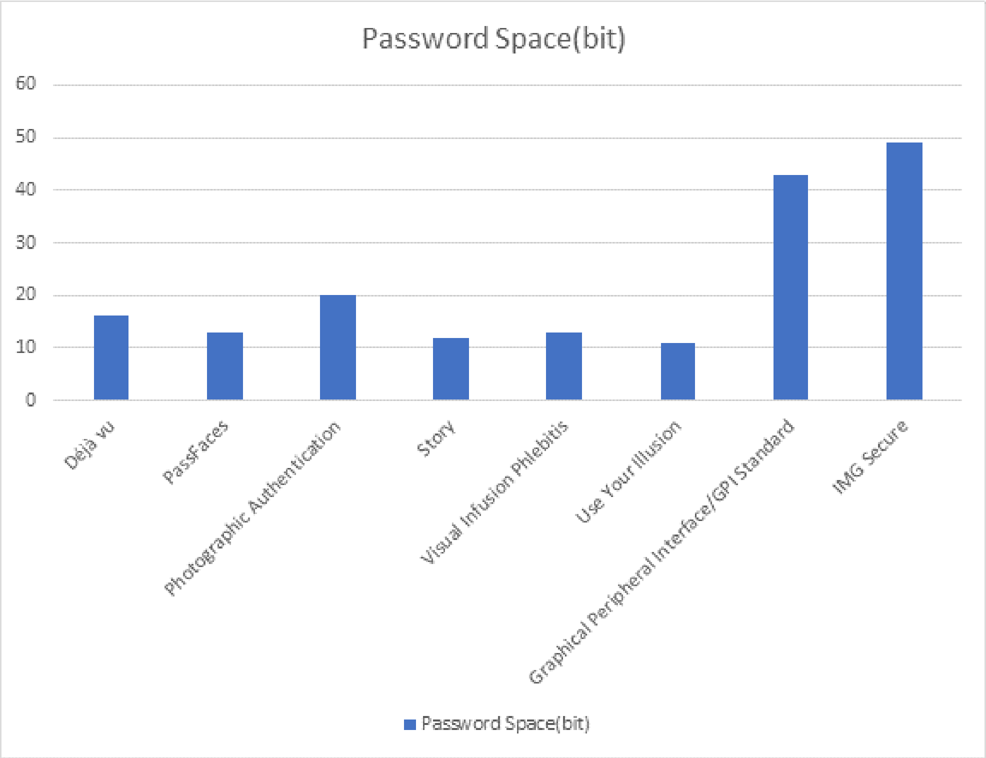


Figure 7: Password Space of Cognometric Schemes

VII. FUTURE WORK

As discussed, the proposed system is safe from most of the attacks, therefore it is perfect replacement for modern day authentication methods of captcha. It can be incorporated in login pages and web applications. The shape of grids can also be changed if the user wishes, such as a triangle, rectangle, circle etc.

Furthermore, the method of securing the passwords in the database can be used with encryption methods such as SHA-256 and validate the hash of the image sequence set received for additional security options.

REFERENCES

[1] B. Kirkpatrick. “An experimental study of memory”.
Psychological Review, 1:602-609, 1894

[2] S. Madigan. “Picture memory”. In J. Yuille, editor, Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[3] A. Paivio, T. Rogers, and P. C. Smythe. “Why are pictures easier to recall than words?”, Psychonomic Science, 11(4):137-138, 1968

[4] R. Shepard. “Recognition memory for words, sentences, and pictures”. Journal of Verbal Learning and Verbal Behavior, 6:156-163, 1967

[5] R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys, vol. 44, no. 4, 2012

[6] D.Sathish Kumar, R.Rajkumar, R.Kalpana. Graphical Image Based Password Authentication System, IJRAR May 2019, Volume 6, Issue 2, 2019

[7] Haichang Gao, Wei Jia, Fei Ye and Licheng Ma. A Survey on the Use of Graphical Passwords in Security. JOURNAL OF SOFTWARE, VOL. 8, NO. 7, JULY 2013

[8] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle. Graphical Password Authentication Using Cued Click Points. ESORICS 2007, LNCS 4734, pp. 359–374, 2007

[9] Chiasson, S., Biddle, R.R., van Oorschot, P.C.: A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS (2007)

[10] Thorpe, J., van Oorschot, P.C.: Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. In: 16th USENIX Security Symposium (2007)