Choice-Based Graphical Password(CGP) Scheme for web applications

Hadier Moawad
Information technology Department
Faculty of Computers and Information,
Menoufia University
Menouf, Egypt
hadier.moawad20@gmail.com

Khalid M Amin
Information technology Department
Faculty of Computers and Information,
Menoufia University
Menouf, Egypt
kh.amin.0.0@gmail.com

Sameh Zarif
Information technology Department
Faculty of Computers and Information,
Menoufia University, Egypt
Data Science Department
Faculty of Artificial Intelligence,
Egyptian Russian University,
Sameh-.Zarief@eru.edu.eg
Sameh.shenoda@ci.menofia.edu.eg

***Abstract*—Today Authentication is an essential mechanism in information security. It was used to identify authorized users and safeguard systems against hackers and spies. A graphical password (GP) is a password that employs graphics rather than text to gain access to computers. The GP is still not widely used in the actual world because users are frustrated by the numerous Login phases and the selection of various determined images from prior techniques, therefore they have returned to textual passwords. The vast majority of research has failed to discover a means to increase overall security, usability, memorability, and login time. In this paper, a novel Choice-Based Graphical Password (CGP) Scheme for Web Applications is proposed. The scheme is a two-level multifactor authentication: textual and recognition. During registration, the user first registered his/her data, and then the system assigned him/her a random and unique number. The second, user chose an image from CGP's dataset or from his/her device. CGP then resized and blurred the user-selected image before encrypting and storing it in the CGP database. The attacker claimed that the image was one element, but it was a combination of five factors (user name, user number, and his/her registered image with the same name, size, and resolution), making it difficult to guess and resistant to several attacks using The Common Attack Pattern Enumeration and Classification (CAPEC). The proposed CGP scheme's performance evaluation enhanced a 36% increase in password space, a 33% increase in possible password numbers, and a 36% increase in entropy when compared to prior methods. Our CGP approach met the challenge of the password being secure, memorable, user-friendly, and time-saving.**

Keywords—Authentication, Graphical Password GP, Choice-Based Graphical Password CGP, Security, User Image UI, Uno. System user Number, NUI 'Registered UI after resizing, Blurring then Encryption ', Password Space PS.

I. Introduction

Authentication is a significant factor in information security. It is the first step to log in to the system, as it confirms that he or she is an Accurate user. The user authentication methods are Token-based authentication (key card, Bank Card, Smart Card), Biometric-based Authentication (fingerprint, Iris Scan, eye scan, etc.), and Knowledge-based Authentication (text-based password, Picture-based password) [1]. Traditional password techniques like textual passwords, also called alphanumerical usernames and passwords, are the most common type of user authentication that refers to using the alphabet, symbols, and numbers as a password to provide user identity and access resources. Textual passwords suffer from less security because of their vulnerabilities to attacks that include dictionary attacks, shoulder surfing attacks, spyware attacks, brute force attacks, and hidden camera attacks. So, graphical password techniques are proposed. To overcome the issues related to textual passwords, textual-graphical password techniques were proposed, which combine both text and graphics to log in to the system. Graphical password schemes have been proposed because pictures are easier to remember than long text. It is referred to as the "*Picture superiority effect,*" and psychology studies found that the human brain is better at remembering and recognizing images than text [2, 3]. If a text password is easy to guess, i.e., if it is less secure and more Usable, otherwise, if the textual password is difficult and long enough to be secure, the user can't memorize it, so GP seeks to balance security, reliability, usability, memorability, and login time. Most studies on security and usability confirm that a system can be secure or usable. There is a high challenge in balancing time, security, usability and memorability. Most of the future Scope seeks to make the system more secure, usable and limit time but most techniques couldn't achieve that balance because, if the technique were secure, it would be time-consuming as it has many images to select and many operations done on it to log in, thus making the system slower and users tired from many images, plus they get confused and tired of registration and many login phases during authentication, then they recur to textual passwords another time [4]. Nearly all research on future work devices involves discovering a method that requires fewer images to be memorized while at the same time being secure. Yet, all papers reduce the image selection from six images to four. They connected security with the number of images selected, believing that whenever the number of images increased, the security increased, but that made users confused and didn't make them prefer graphical passwords. In our scheme, we seek to produce a novel scheme that reduces the number of images from four to one image as a minimum to three tree images as a maximum. Based on user desire, our scheme gives the user the privilege to choose the level of security he wants. If he or she prefers the first level, choose one image; if he or she prefers the medium level, choose two images; or choose a tree image. It's a challenge for the users to memorize many numbers of images every time they sign in. So, our choice-based graphical password CGP is proposed to balance security, memorability and usability in addition to time reduction. Our CGP increased usability by reducing the number of images, thus increasing memorability and reducing time. In addition, our CGP designed a method during the process of storing the user portfolio to increase security, but that was done implicitly inside the system without forcing the user to do any transactions. The user could choose his or her image easily, thus increasing security, reliability, and usability.

on the opposite, the other methods constrain the user to select many images or perform many operations on them, putting a workload on the user to memorize many images and often forgetting some pictures. thus, increasing security but increasing login time and reducing memorability. GP is more secure than a textual password, but GP is vulnerable to attacks like social engineering, shoulder surfing, spyware, educated guessing, sniffing, phishing, dictionary attacks, and many others [5]. The rest of the paper is organized as follows: In Section II, we review some graphical password-related works. Section III presents the proposed Choice-Based Graphical Password method. Section IV shows the design details of the proposed work. Section V mentions the experimental results of the proposed method. The last section, Section VI, shows the paper's conclusion and future work.

II. Related Work

A lot of research has been done on graphical password techniques. Originally, it was introduced by Blonder in 1996 [6]. The picture-based password, or GP, is a type of knowledge-based authentication system. Recognition-based techniques are a type of GP that uses images as a password to access the system. GP has two stages: Registration and Authentication. There are three types of graphical password techniques: recognition-based, pure recall-based, and cued recall-based. In the Recognition-based technique, during the registration process, the user selects several images from a set of images presented in a graphical user interface (GUI). So, a graphical password is sometimes called Graphical User Authentication (GUA) [5]. GUI produced by the system During the Authentication process, the user must recognize the selection he previously selected during the registration step [1, 6–10]. In the second type, pure recall-based, the user must produce his graphical password, which he generated in the registration phase. In this case, unlike the previous type, the user needs to reproduce his password without any given reminder, Such as drawing a particular shape. In contrast, in cued recall-based systems, several specific locations within an image can be selected as the graphical password [9, 11–13]. There are many examples of GP techniques. In the registration step, the user selects at least five categories; accordingly, he or she selects images for each category as his password [4]. Later on, in the authentication step, the user must select the password-selected images he previously selected on the registration step. In other research, in the registration step, Participants were required to memorize two system-assigned images, then select 4 categories to select 4 images as their password. In which participants were only allowed to choose one image per category. After the information is submitted to the database, the user Creates secret clicks for the chosen images and then confirms his clicks on the same spot [14]. The most common technique used in GP is the pass face, as users can remember faces better than images. At first, users selected 4 images from 3*3 grid images. To force it, increase the number of images selected to 5 and the image grid to 25 images, but it took a long time and it was easy for malicious to look at the mouse device when entering the password [15]. In S. Gokhalea approach [16], in the registration step, 25 images are presented to the user. These images are common to all users. The user has to select a number of images to set as a password. The user can repeat any image. Now he/she is presented with a question set and these images. The user has to select any three questions from this set. To answer a question user has to click on any point on the image. for the three questions, there will be three different points. The individual point is called ROA (Region-Of-Answer). So there are three different ROAs. In authentication, the user entered the username and two selected images from 25 images. In the Vaddeti approach [17], in the registration stage, the user registered his/her profile then the system took the user ID and converted it into two images by using the visual cryptography concept: one image was sent to the user's e-mail, which was called user share, and the other was sent to the server, which was called server share. Then the user must select four images from a 5-by-5 grid. In authentication, the user entered the user share, and after the system combined the user share with the server share, the user should select the four images he or she predefined in the registration stage. This method is nearly considered the first recognition method that suggested reducing images to four images and changing the concept of thinking that when increasing the images selected, the security increased and suggested a good idea to keep the system secure, but it also could be hacked and took a long time, it couldn't achieve the challenge of increasing the tree factors, Security, memorability, and usability. Many types of research are based on the selection of images, or making any click then selecting images in authentication, which makes GP vulnerable to attacks. In addition to, users are tired of the number of processes of registration and authentication, and there are many categories that lead to people not using the GP and preferring the textual password. we propose a novel CGP scheme to make GP easier as the user chooses only one image as a medium level of security to be memorable and reduce the login time while at the same time maintaining the security of the system. If the user wants a higher level of security, they choose two or three images thus making CGP more reliable for users.

Nearly no new approaches or schemes on GP for web apps were done between 2016 and 2020, and researchers preferred to use GP in cloud computing and mobile computing instead [18–24]. They tended to improve the GP for cloud services and web applications start in 2020 [1, 18,19, 22–29].

Cloud computing is an internet service environment using shared information, resources, software, and hardware per user's demand or company's request to access their data from anywhere or at any time. So, The GP schemes used for web applications can be used for cloud computing to successfully authenticate users before they take the privilege to access their resources or data [1, 18–19, 22].

Mobile devices are personal communication devices used to store users' confidential information to perform their activities on social networks, emails, and personal Internet banking entertainment. They used a biometric password, but it can be hacked by spoofing. Because of the weaknesses of PIN, PATTERN, and biometrics, the researchers swung to GP as an alternative [19–21, 25]. Olade [20], they present a SemanticLock for touchscreen-based mobile devices that uses pairs of icons to create a semantic story that represents the password, and in Andriotis [21], the password is a sequence of shapes from a set of symbols (O, squares, triangles, and Times). The user's generated password must be from 4 to 9 shapes and contain two different shapes. They recommended enhancing usability and memorability. They can be attacked by shoulder surfing. There are five methods to access authentication services and cloud computing.

i) simple password; ii) graphical password; iii) Biometric password; iv)third-party authentication; v)3D password object [18]. According to a survey done on users authenticated by all five levels of authentication, they sent their views on They observed that when using a multi-level password, it increases the password security and reduces password breaking, but it also increases the user's frustration [18, 19, 27, 28]. The 3D password object and third party are not supported on it, and the biometric isn't preferred because of the user's personal characteristics changing [19, 26]. In Mrs. Patil [18] and Al-Shqeerat [19], they found that using recognition techniques has less password space than textual passwords. So they suggested using combinations of passwords.

In Mrs. Patil [18], they used three levels of authentication: textual, biometric, and GP, to overcome the password limitations, but it irritated the users, so they recommended using fewer levels of authentication. Al-Shqeerat [19] used hybrid graphical schemes, recognition, and recall-based techniques. They used three factors for authentication that the user had to verify with each other. At registration, the system displays a grid of images in random order, each related to a question. The user clicks on a part of the selected image called a hotspot to answer the image. At authentication, the user has to pass the three levels to log in successfully. The user must select his or her image and choose the predefined secret question from the system's suggested questions, then click on his or her hotspot to answer the question. These methods take a long time and can be hacked when users click and answer. They made a questionnaire and found that 94% found it easy, 63% could remember the password, and only 9.89% of participants found it boring. This methodology was conducted to investigate the user's satisfaction, usability, login time, and performance [19]. In Abhijith [22], at registration, the user enters a picture and then chooses regions in the images called POI. The system represents the POI with a circle; this POI can be ordered or random, and then the user either writes a text inside or quits. This methodology introduces a very large PS as it is a combination of (GP, text, POI number, and POI order). Precisely, we can't calculate its PS as the user can enter a large number of POI with any order, write any text, or leave it empty.

In Carrillo-Torres [29], at registration, the proposed MFA mechanism requires users to complete all configuration processes. First, the user creates an account (with a unique username, password, and email), then the user is required to upload irredundant 9 images (at least 20) and is recommended to enter an image of his/herself. The user must create at least 5 own relations between registered images. When it has 10 relations, write this relation in a text field. Every image should be related to another, and there isn't an image that is related to itself and doesn't have a relationship with others.

At login, the user must enter his/her correct name and password, and then the system shows a grid that has 12 random images from 500 and contains 4 of the user's images, which he/she uploaded during the configuration process. Once the user selects the four images successfully, the system shows them in a grid, and the user must choose two images and then select the relationship between them. If the user fails in any step, the authentication attempts fail. Prior to user testing and questionnaires, only 70% of users had successful authentication, and only 45% decided to use this mechanism instead of others. Users approving that mechanism are sometimes usable and applicable; it is difficult and takes a long time, but it is secure as it achieves a larger password space [29], but it would be hacked by shoulder surfing attacks and hidden cameras when the user inserts the images and chooses which two related images to use, and attacked by dictionary attacks and spyware/key logs where the user writes those relations.

The GP has been widely used in deep learning, the internet of medical things, and car security for driving seats [30, 31].

The Pass-Face technique is a weak GP as it has a short password space, but it is nearly the most preferred GP from users as the faces can be remembered easily compared to other images [19], so we used it in our comparison to prove our CGP usability and memorability.

The cued recall is less usable than recognitions, but it's more secure because of its strength and large password space [1, 3, 9, 18, 19, 22]. So, we used a recall technique by S. Gokhalea [16] to prove our CGP security compared with the recall techniques and Vaddeti [17] as a recognition technique.

We compare our scheme with these three approaches: Pass Face [15], S. Gokhalea [16], and Vaddeti [17], as shown in Table 2.

III. Proposed CGP Algorithm

The proposed choice-based graphical password CGP method follows the category of recognition-based Techniques.

- The system architecture of the proposed choice-based graphical password scheme is shown in Fig. 1.

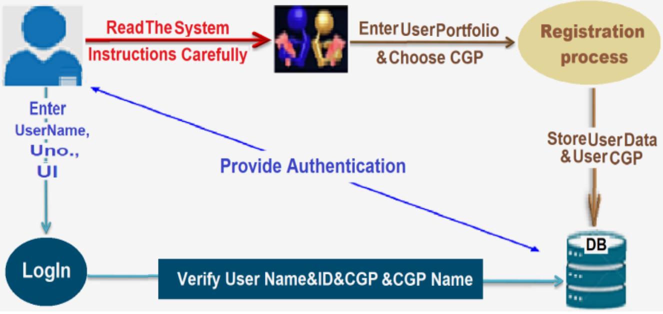

Fig. 1: The system architecture of the choice-based graphical password scheme

In the proposed CGP scheme, before the registration step, users should read the system instructions carefully, which explain to the user the use of the proposed CGP and warn him/her to be attentive to the instructions during the steps of the registration process as the system doesn't send these via email or SMS. These instructions make the CGP more complex and not to be hacked during the login process. The CGP Registration process has two steps. First, the user registers his/her profile data and second, he/she must choose at least one image that would be a part of his/her personal CGP password after the system does some operations on it. The user image chosen is called "UI". The system called the first-choice user Image called "UI_1". The CGP doesn't force the user to choose an image from the system dataset as other methods, but he/she can choose from his/her device to memorize it easily. If the user wants to increase the level of security, he can choose two or three images called "UI2" and "UI3". Every time the user login, he/she must choose the same image he predefined in the CGP registration stage with the same dimension and the same name. The CGP uses the UI dimension to create the user CGP password by performing some operations on it and transforms the UI to a new user image, "NUI" which is stored on the CGP database. The NUI and the image name are part of the CGP password. After the user confirms his/her username and his/her UI, the system gives him/her a random and unique number that is shown on the screen for a few seconds and then hidden. This number was also part of the CGP. Thereby, the registration process was finished successfully, as shown in Fig. 2. and the user isn't applicable to memorize only one favorite image he/she preferred to choose during the CGP registration stage instead of at least five images as discussed before in other methods. In addition to the favorite name, he also suggested the representation and the number the system gave.

The proposed CGP is responsible for creating a complex password for the user, contrary to the previous methods that forced users to select many images from determined images of the system dataset or produce any operation on system images to increase security. The complex CGP password consists of a combination record containing the values of the user's name, system user number, new user image, and user image name. The CGP format is a list in the form of [UserName, SystemUserNo, NUI, UI Name].

In the CGP authentication process, users go through login stages based on the user images chosen in the registration. If the user chose level 1, he/she chose one image to log in, and so on in other levels, level 2, and level 3.
At first, the user enters his/her name and the suggested user number from the CGP system. If the user is authorized successfully, he/she must enter or choose his/her UI during in the registration from his/her device or from the system dataset. The UI must have the same dimension and name, i.e., the user should choose the same image with the same name, not an image with similar data, as the CGP system depends on the image details. If authenticated, the user is allowed to log in to the CGP system.

A. Registration Process

The registration process includes the following steps:

1. In the first step of the CGP registration process, a user creates his/her profile details, such as user name, email, mobile number, age, and Gender.
2. The user should read the instructions carefully shown by the CGP system.
3. The user chooses a level of security: if he/she chooses level 1, he/she chooses one image; if level 2, chooses two images; and if level 3, chooses three images.
4. The user chooses an image he/she prefers from the CGP system dataset or from his/her device, the CGP calls it 'UI' and stores it in the CGP DB, the user can memorize preferred images more than those introduced by the system, which is the opposite of the other methods that force the user to select images from the system, and makes the user confused and forget the pictures many times.
5. The CGP scheme has done some operations on the UI to be complex and secure from hackers or spies.

6. After the user confirmed his/her data, The CGP system generated a random and unique number and gave it to the user, which was shown on the screen and then removed. The suggested system user number wasn't sent to the user so that it wouldn't be hacked by internet media tools.

The final record for each user in the CGP DB contained the user name, system user number Uno., NUI 'Registered UI after resizing, Blurring then Encryption, UI name, and UI.

Nearly all techniques were supposed an image size of 200X200 but CGP imported any UI size from the user either big or small then resized it and made the following operations:

At first, the CGP resized the image from the user device or system dataset to 200 x 200.

The resized image was cropped to be 5X5, therefore the ROA is 5*5=25.

The cropped image was blurred using Gaussian Blur.

The Blurred image had been encrypted using the A-Es encryption technique.

The encrypted output image was called 'NUI' and stored on the CGP DB for each user record.

B. Authentication and Login process

During the Login and authentication stage, the login undergoes two phases:

1. The user enters his/her name and the system number he gave from the CGP system. After confirming the registration stage, the CGP locks the keyboard so as not to be hacked by attackers, If authorized successfully, he/she enters the second login phase.
2. The user chooses the UI he/she chose in the registration stage.

If the first login phase fails and the user gives three attempts, then the CGP system is blocked for half an hour.

If the first login phase succeeds but the second login phase fails, the user takes another three attempts, and then the system destroys three hours, sends a message to the user's email for verification, and resets the password. If he/she had chosen level 2 or level 3, he/she is disturbed to choose all UIs from the start another time.

3. The CGP exports the user data: the user's name, the user system number, the UI's, and the UI's name. Then, the same operation was made on the user UI entered to compare that record with the others that had the same user's name and user system number in the CGP DB; if they were similar, the user could log in and access the next page.

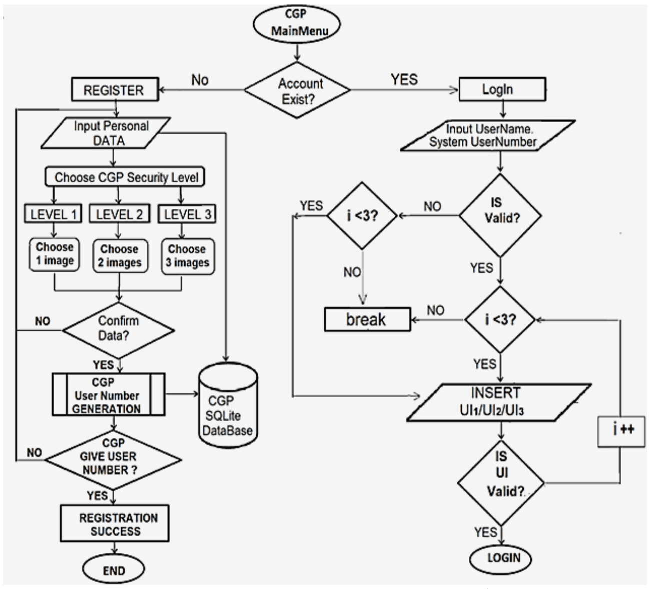

Fig. 2: Registration and Authentication block diagram of the proposed CGP

IV. Experimental Study

In previous methods, the user had to choose the same five images or more he selected in the registration phase; therefore, the system is more prone to spying, but the proposed idea of the CGP components makes the password more complex and difficult to guess because of the CGP password format, which depends on a combination of the UI name, a part of the UI in addition to the user's name, and the suggested system user number, all match each other.

A. Dataset Description

Any recognition-based graphical authentication system largely depends on the image dataset. The password consists of images, so the dataset plays an important role in GP. Users should choose the CGP image carefully based on the category he/she prefers to memorize the CGP password easily or choose the personal image they want on their device.

Each category holds inside it a group of images. When the user chooses a determined category, the CGP system shows the category-related images.

The CGP's dataset consists of 2000 images in various categories, as described below:

1. Football dataset: this dataset includes the football team’s name, football t-shirts, football player’s name, and football country flag.
2. Country dataset: it contains something connected to countries such as places, human faces, flags, and popular personalities like food or clothes.
3. Age dataset: based on user age, the system presents images like youth, kids, adults, or teenagers.
4. Gender dataset: if male, the system session presents cars, sports, and video games if female, the system session presents clothes, makeup, accessories, Toys, or television shows.
5. Job dataset: like an engineer, doctor, teacher, student, and more.
6. Robots, flowers, trees, plants, University, car brands, food, hobbies, famous people, dressing style, traffic signals, alphabet, clothes, colors, and more categories.

B. Description Table of CGP Components

The proposed CGP scheme has 10 parameters as shown below in Table 1:

Table.1 The Notation Description of the Proposed CGP

No.	Item	Description	Value
1	R	The number of rounds	**From 1:3**
2	UI	User Image	**From 1:3**
3	Uno.	CGP System User Number	**Using six digits out of 0-9**
4	N	Total number of Images	**49**
5	N**i** **'k'**	Number of chosen Images per Login session **from i=1 to i=3**	**i= 1:3**
6	**W, H**	W number of rows, H number of columns	**7,7**
7	**X, Y**	X*Y is the dimension of 'UI '	**200*200**
8	**ROA**	Z*Z is the dimension of the cropped UI	**5*5**
9	**UI$_1$,** **UI$_2$,** **UI$_3$**	UI**1**first user Image chosen, UI2 second User Image Choiced, UI**3** Third User Image Choiced.	
10	**NUI**	UI after resizing, Blurring then Encryption	

C. Experimental Setup

The experiment's configuration was developed using a development tool (PAYTHON/ASP.NET), programming language (PAYTHON), and database (SQLite), which run from PC/Laptop.

V. Results and Analysis

To date, the GP is not widely used in the real world; only the pass-face technique is used in many systems. so, research is still being done on it to make it reliable and give confidence to the user to select the GP [17].

The success rate of any GP system depends on its security, reliability, memorability, usability, speed, time, and password entropy [17, 18]. The three main factors of GP are Security, usability or memorability, and time. Nearly all paper research focuses on the problem of balancing between the three factors, and it is still a challenge for future researchers to propose a methodology that strengthens the three factors [17]. The proposed CGP scheme goes ahead in balancing between these three factors as shown in Fig. 3.

The security of the methodology used leads to reliability. If the system used is secure, it will be confident and reliable for the user; if the methodology is used easily and gives a user a domain to choose from over a wide area and doesn't force the user to choose a determined number of images, this usability leads to more memorability, and if the system process is executed fast, the time will decrease. Thus, the system has achieved a high success rate in overcoming the drawbacks of GP problems and our CGP achieved the three-factor challenges as shown in Fig. 3.

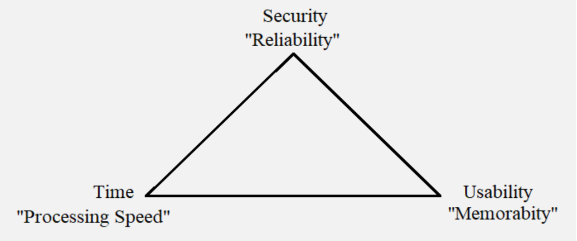

Fig. 3: The Three Metric Factors of the Proposed CGP Scheme.

A. Security and Reliability Analysis of Proposed CGP

A security entity protects the system from inside and outside dangers like attackers, spies, threats, and others. It's a metric factor used to measure the strength of the system or methodology used. The security level of CGP was measured based on three factors: the strength of defiance against attacks, Password space, and Password entropy. When the proposed system has a combination of two types of passwords, it provides strong security against attacks [6].

Password Space (Ps)

The **Ps** is the complexity of the password, and it is a measurement of the total number of possible passwords that can be created by a combination of a number of possible password images. It is a very large number a person can imagine, so it cannot be cracked easily. Such numbers are a bit unwieldy, and the entropy is defined as a binary logarithm of these values. It was generated by combining k chosen images from N images for all images. Whenever the password space was higher and whenever the password security and strength were increased against brute force, guessing attacks, and other attacks, the probability of the attacker guessing random passwords depended on the number of possible passwords. If the technique used a combination of two types of passwords, the **Ps** = Ps1* Ps2, as discussed in Equations [1:6], which provides a huge Password Space because there are millions of possible passwords, thus making the system more secure [4, 17, 18, 20].

All past algorithms used 25 images and a user-selected number of images out of these images. Our CGP process was to maximize these numbers to 50 to increase the search area and make it difficult for the attacker to guess the password, but we used 25 images in equations like past algorithms to make a fair comparison, as shown in Figure 4.

There wasn't a determined formula for SP or calculating the possible passwords, as there were many methodologies of recognition techniques and each needed different requirements, but it mainly depended on the row size [18]. We can measure the Ps using the algorithms [18, 20, 22, 23, 24] that calculate the Ps using two equations.

The first equation calculates the number of possible passwords Ps1 for choosing k images from N images.

When the methodology used is a recognition-based technique only without image randomization on the grid, the Ps1 is calculated as shown in Equation 1 Case 1, and if there is a random image shuffling, the Ps1 is calculated as shown in Equation 1 Case 2 [16].

If the methodology used is hybrid, i.e., a combination of recall and recognition techniques, the Ps1 is calculated as shown in Equation 1 Case 3, and if it is a combination of recognition and textual techniques, the Ps1 is calculated as shown in Equation 1 Case 4 and R equal 1.

In the recall-based technique, the user reproduces the C pattern either by drawing or clicking on the selected image, so the Ps1 is calculated as shown in Equation 1 Case 3 [16, 26].

$$Ps_1 = \begin{cases} \binom{N}{k} & \textit{Case } 1 \\ N! \times \binom{N}{k} & \textit{Case } 2 \\ C \times \binom{N}{k} & \textit{Case } 3 \\ N^k & \textit{Case } 4 \\ N^k \times \binom{N}{k} \times R & \textit{Case } 5 \end{cases} \qquad (1)$$

In a textual password, the Ps depend on N symbols and password symbols k, and the total number of possible symbols available is calculated as shown in Equation 1 Case 4. The CGP used numbers (0:9) only on T symbols and then assigned an identified number to each user registered, using six digits out of 0–9. The CGP depends on the relation 'R' of the five factors of its components together, R=5, CGP Ps1 is calculated as shown in Equation 1 Case 5.

The second step of authentication depends on the image size; if the methodology is working on the whole image selected, the Ps2 is calculated as shown in Equation 2 case 1, and if it is working on a region of the image selected, the Ps2 is calculated as shown in Equation 2 case 2.

If y is the total number of images, Z is the password size, and x is the maximum number of selected images, the Ps2 is calculated as shown in Equation 2 case 1[18].

If the methodology depends on a region of image area to work (ROA), and X, Y are the image sizes, Z is the ROA, and q is the number of questions, clicks, or maximum selected image numbers, then the Ps2 is calculated as shown in Equation 2 case 2[16].

$$Ps_2 = \begin{cases} \displaystyle\sum_{z=1}^{X} \binom{y+z-1}{y-1} & \textit{Case } 1 \\ \displaystyle\sum_{i=1}^{q} i! \times \left(\frac{x \times y}{z^2}\right)^{i} & \textit{Case } 2 \end{cases} \qquad (2)$$

The Password Space (**Ps**) = Ps1* Ps2 and Ps1 with random images, While the Ps is increased, the security of the methodology used is increased, and the CGP proposed is the most secure technique, as shown in Table 3. and Fig. 4.

Table.2 The Comparison Methodologies and their GP Technique Used

Methodology	**GP Technique used**
Pass Face[15]	Recognition only
S. Gokhalea [16]	Recognition + Recall 'Click'
Vaddeti [17]	'Image'+ Recognition
CGP proposed	'Random No. ' + Recognition

Table.3 The Password Space Based on Equation 1, 2.

Methodology	Ps1	Ps2	Ps
Pass Face [15]	8.24e+29	1.42505e+5	1.195e+34
S. Gokhalea [16]	1.39e+28	6.051e+4	8.43e+34
Vaddeti [17]	8.9e+28	2.3746e+4	2.11e+33
CGP (1 image choice) CGP (2 image choice) CGP (3 image choice)	1.94e+34 2.325e+34 1.875e+35	2.458e+10	4.769e+44 5.715e+44 4.609e+45

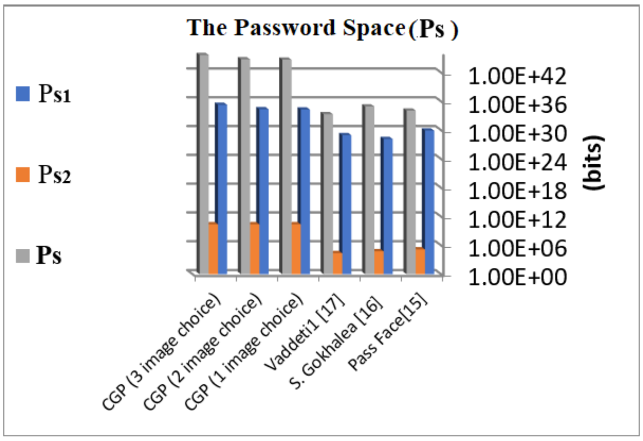

Fig. 4: The password space of the Comparison Methodologies as shown in Table 2.

A. *Usability and Memorability Analysis of Proposed CGP*

Whenever there are a large number of passwords, the probability of guessing the correct password decreases, making the attacker unable to guess the password. There isn't a predefined formula for calculating the probability of Guessing the correct user password chosen during registration, but we used the algorithms [4, 23, 24], and we can calculate it by Equation 7.

The CGP number of password images was high, so the probability of guessing the password was low; the attacker couldn't guess a password from millions of possible passwords. So, the usability is high, and the system is more secure than past methodologies, as shown in Table 4 and Figure 5.

B. *Probability Of Guessing the Correct User Password*

The Probability of Guessing the correct user password is given according to equation 1 case 4, This case is the number of possible passwords.

- ***probability of guessing the correct user password***

$$P_1 = \frac{1}{(N)^k} \qquad (3)$$

- The password Entropy is the strength of the password and the difficulty of guessing it and is the binary logarithm of the password space when the binary logarithm can be read as the number of bits required to express the number. The higher the number of possible passwords, the lower the probability of guessing the password and the greater the CGP entropy, as shown in Table 4.

Table.4 The Password Number and its Probability according to Equation 3.

Methodology	**Password number**	**P_1**
Pass Face [15]	9.77E+06	1.024e-7
S. Gokhalea [16]	1.88E+03	5.33e-4
Vaddeti [17]	3.91E+05	2.56e-6
CGP proposed	1.56E+10	6.4e-11

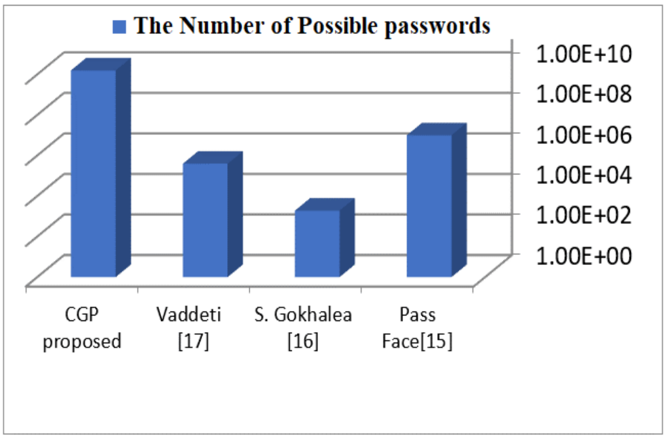

Fig. 5: The password Numers of the Comparison Methodologies as shown in Table 4.

C. *Processing Speed and Time Analysis of the CGP Scheme*

The number of login rounds in CGP decreased, so the login time increased. In nearly all approaches introduced, users suffer from the long login time, so they recommend modifying or innovating a methodology to enhance time and be as user-friendly as possible.

D. *Possible Attacks on the CGP Scheme*

The attacks on recognition-based graphical password techniques have been identified by the Common Attack Pattern Enumeration and Classification (CAPEC) and classified into six attacks: dictionary, brute force, spyware, guessing, social engineering, and shoulder-surfing [19], in addition to phishing and sniffing Attacks.

D.1 Dictionary Attack

In which the attacker makes a list of user passwords he/she chooses and then attempts to hack the system. It depends more on keyboard input than mouse clicks. Textual passwords are more vulnerable to this attack than recognition-based passwords that depend on the mouse to choose the password. If the number of expected CGP guesses and the password space were reduced, the success ratio of the attack would increase. The pass-face algorithm is the only GP technique to suffer from dictionary attacks [17, 18]. In the proposed CGP scheme, in authentication process one, the user inputs the system user number, so it can be hacked, when The CGP is a combination of four parameters and doesn't depend on that number alone, it isn't vulnerable to dictionary attacks.

D.2 Brute force attack

It works like the dictionary attack we explained in Part D.1. It also depends on reducing the password space and the probability of guessing the correct CGP Password.

Because recognition-based graphical passwords depend on mouse clicks, it would be difficult for the attacker to monitor the password unless the attacker's programs innovate an accurate mouse motion automatically to record the user's GP input [17, 18]. Thus, the CGP proposed scheme prevents brute-force attacks.

D.3 Spyware attack

It is software or tools installed for monitoring the user's screen input. Any movement of the user's mouse or key is recorded by this malware. Spyware attackers use spy cameras to record user data. Previous research proves that screen monitoring and keylogging spyware are not enough to crack the GP as they require additional data such as time, window size, and position [17, 18, 20, 21]. The CGP depends on UI dimensions plus the combination of the three items we discuss, it's difficult for spyware to hack.

D.4 Guessing attack

Since users choose their passwords based on personal data, the attacker can guess them using possible probabilities, and previous researchers have found that GP can be easily guessed by attackers [18]; they advise users not to use personal images, but CGP gives the user the privilege to choose any image he/ she prefers, whether it is personal, well-known to others, or not. As the CGP depends on image size, visibility is determined and clarified, the combination of the image name, user number, and user name, and shows the UI as blurred to prevent the educated attack, it is not vulnerable to attack even if the guessing attacker knows the user image.

D.5 social engineering attack

Social engineering is a type of criminal that cogence people to confidence to get confidential information like phone calls to give up a password or bank information [17]. The proposed CGP scheme restricts the users in the system instructions before registration that the number the system gives is not known and no one will request or call to know it, and it will be difficult for GP to send images in SMS.

D.6 shoulder-surfing, hidden camera attack

It refers to capturing the user's information by direct watching, over the victim’s shoulder, or recording the user's authentication session while choosing or producing the images as a password. GP is more sensitive and vulnerable to shoulder surfing attacks [1, 4, 6:13, 17, 18]. Even if the attacker used external recording devices such as a hidden camera, video camera, or high-resolution camera to obtain the user-input CGP image during registration or authentication, it would be difficult to trick it as the proposed CGP hides mouse clicks and shows blurred images during registration and does not show them during authentication.

D.7 Phishing, sniffing, and wiretapping Attacks

Phishing websites are designed to trick user's credentials into disclosing personal or financial information, usually by creating a copy of a legitimate website. These false websites aim to redirect a legitimate website's traffic to a fraudulent website. Sniffing attacks allow for the capture of sensitive user data when it is transmitted through media channels, public networks, and/or is unencrypted. The proposed CGP prevents sniffing attacks as it doesn't send the system user number to the user either in an SMS or via email and it encrypts a cropped part of the UI, not the entire UI.

VI. CONCLUSION AND FUTURE WORK

This paper proposes a two-level multifactor authentication CGP scheme for web applications that can also be used for cloud services and models. We presented a novel CGP scheme based on a combination of two authentication techniques, textual and recognition, to decrease the limitations of textual and recognition when using each one alone. In this study, we achieve the challenge of developing a highly secure, memorable, and usable GP, decreasing the time and Categories used as users are tired of registration and Authentication processes, and giving users the privilege to choose any personal image they prefer. The proposed method is based on a combination of multiple factors (username, user number, image name, image size, and image resolution); if any factor changes, the authentication fails. When the attackers monitor the login process, they only observe the user image, and they aren't aware of the relations between all factors, the CGP scheme is resistant to several attacks. The only drawback of that scheme is that it needs an educated user, but if the user trained successfully, there wouldn't be any problems with it. To evaluate the proposed CGP scheme, we use several metrics that calculate the probability of guessing a password, the password space, and the entropy to compare it with the recognition and recall technique to prove its strength and accuracy, regardless of whether they only use one metric to measure their approaches. The results showed that the proposed CGP scheme had a higher password space and a higher number of possible images than all other comparison approaches, and it couldn't be predicted or hacked. The proposed CGP scheme enhances the possible number of images from 1.88E+03 to 1.56E+10, the password space from 2.11E+33 to 4.109E+45, and the password entropy from 5.33E-4 to 6.4E-11. The future scope of this CGP study includes checking whether the proposed CGP scheme is feasible for all users and developing a new secure and strong GP by replacing the text with another method to increase usability and password space for use in ATMs, mobile phones, and applications. In the future, we will study how to use GP in IoT, Health Care, driving, and deep learning.

Table 5 Comparison of Security and Performance Based on the Study in Pass Face [15], Vaddeti [17], and the proposed CGP Scheme.

ATTRIBUTES	**Pass Face [15]**	**Vaddeti [17]**	***CGP proposed Scheme***
Sensitive to Shoulder surfing attack	YES	NO	NO
Sensitive to hidden camera attack	YES	YES	NO
Sensitive to guessing attack	YES	YES	NO
Sensitive to brute force attack	YES	YES	NO
Sensitive to phishing attack	YES	YES	NO
Sensitive to Dictionary attack	NO	NO	NO
User-Friendly	NO	NO	YES
Easy To Remember	NO	NO	YES
Fast Excution	NO	NO	YES

REFERENCES

[1] Anitha, H. M., & Jayarekha, P. MultiStage Authentication to Enhance Security of Virtual Machines in Cloud Environment. International Journal of Advanced Computer Science and Applications, 12(10), (2021).

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

[3] Mishra, A., Jadhav, R., & Patil, S. A Shoulder-Surfing Resistant Graphical Password System. International Research Journal of Engineering and Technology (IRJET), 2018.

[4] Alesand, Elias, and Hanna Sterneling. "A shoulder-surfing resistant graphical password system.", 2017.

[5] Blonder, G. "Graphical Passwords. United States Patent 5559961, Lucent Technologies." Inc., Murray Hill, 1996.

[6] Suo, X., Zhu, Y., & Owen, G. S. Graphical passwords: A survey. In 21st Annual Computer Security Applications Conference (ACSAC'05) (pp. 10-pp). IEEE,2005.

[7] Biddle, R., Chiasson, S., & Van Oorschot, P. C. Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 1-41, 2012.

[8] Dunphy, P., Heiner, A. P., & Asokan, N. A closer look at recognition-based graphical passwords on mobile devices. In Proceedings of the Sixth Symposium on Usable Privacy and Security (pp. 1-12), 2010.

[9] Osman, Mohd Zamri, and Norafida Ithnin. "Category-Based Graphical User Authentication (CGUA) Scheme for Web Application." Pattern Analysis, Intelligent Security, and the Internet of Things. Springer International Publishing, 2015.

[10] Goldberg, Joseph, Jennifer Hagman, and Vibha Sazawal. "Doodling our way to better authentication." CHI'02 extended abstracts on Human factors in computing systems. 2002.

[11] Yeung, Andrew Lim Chee, et al. "Graphical password: Shoulder-surfing resistant using falsification." 9th Malaysian Software Engineering Conference (MySEC). IEEE, 2015.

[12] Jali, M. Z. A study of graphical alternatives for user authentication (Doctoral dissertation, University of Plymouth), 2011.

[13] Meng, Y. Designing click-draw-based graphical password scheme for better authentication. In IEEE Seventh International Conference on Networking, Architecture, and Storage (pp. 39-48). IEEE, 2012.

[14] Brostoff, S., & Sasse, M. A. Are Passfaces more usable than passwords? A field trial investigation. In People and Computers XIV—usability or else! Proceedings of HCI 2000 (pp. 405-424). Springer London., 2000.

[15] Towhidi, F., Masrom, M., & Manaf, A. An enhancement on Passface graphical password authentication (Doctoral dissertation, Universiti Teknologi Malaysia),2010.

[16] Gokhale, M. A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. Procedia Computer Science, 79, 490-498., 2016.

[17] Vaddeti, A., Vidiyala, D., Puritipati, V., Ponnuru, R. B., Shin, J. S., & Alavalapati, G. R. Graphical passwords: Behind the attainment of goals. Security and Privacy, 3(6), e125, (2020).

[18] Patil, D., & Mahajan, N. An analytical survey for improving authentication levels in cloud computing. In 2021 International Conference on Advanced Computing and Innovative Technologies in Engineering (ICACITE) (pp. 6-8). IEEE, 2021.

[19] Al-Shqeerat, K. H., & Abuzanouneh, K. I. A hybrid graphical user authentication scheme in mobile cloud computing environments. International Journal of Communication Networks and Information Security, 13(1), 68-75, 2021.

[20] Wang, S., Salehi-Abari, A., & Thorpe, J. PiXi: Password Inspiration by Exploring Information. arXiv preprint arXiv:2304.10728, 2023.

[21] Andriotis, P., Kirby, M., & Takasu, A. Bu-dash: a universal and dynamic graphical password scheme. In International Conference on Human-Computer Interaction (pp. 209-227). Cham: Springer International Publishing, 2022.

[22] Edward, A. L., Suru, H. U., & Okudo, J. Position-Based Multi-Layer Graphical User Authentication System. American Journal of Software Engineering and Applications, 11(1), 1-11, 2022.

[23] Constantinides, A., Belk, M., Fidas, C., Beumers, R., Vidal, D., Huang, W., ... & Pitsillides, A. Security and usability of a personalized user authentication paradigm: Insights from a longitudinal study with three healthcare organizations. ACM Transactions on Computing for Healthcare, 4(1), 1-40, 2023.

[24] Dias, N. I., Kumaresan, M. S., & Rajakumari, R. S. Deep learning-based graphical password authentication approach against shoulder-surfing attacks. Multiagent and Grid Systems, 19(1), 99-115, 2023.

[25] Bartłomiejczyk, M., & Kurkowski, M. Multifactor authentication protocol in a mobile environment. IEEE Access, 7, 157185-157199, 2019.

[26] Conroy, T. B., Hui, X., Sharma, P., & Kan, E. C. Heart ID: Biometric Identification Using Wearable MIMO RF Heart Sensors. IEEE Journal of Electromagnetics, RF, and Microwaves in Medicine and Biology, 7(1), 3-14, 2022.

[27] Lone, S. A., & Mir, A. H. A novel OTP-based tripartite authentication scheme. International Journal of Pervasive Computing and Communications, 18(4), 437-459, 2022.

[28] ALSaleem, B. O., & Alshoshan, A. I. Multi-factor authentication to systems login. In National Computing Colleges Conference (NCCC) (pp. 1-4). IEEE, 2021.

[29] Carrillo-Torres, D., Pérez-Díaz, J. A., Cantoral-Ceballos, J. A., & Vargas-Rosales, C. A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User-Established Relations. Applied Sciences, 13(3), 1374, 2023.

[30] Khan, M. A., Din, I. U., & Almogren, A. Securing Access to Internet of Medical Things Using a Graphical-Password-Based User Authentication Scheme. Sustainability, 15(6), 5207, 2023.

[31] Azadani, M. N., & Boukerche, A. Siamese temporal convolutional networks for driver identification using driver steering behavior analysis. IEEE Transactions on Intelligent Transportation Systems, 23(10), 18076-18087, 2022.

[32] Khodadadi, T., Alizadeh, M., Gholizadeh, S., Zamani, M., & Darvishi, M. (2015). Security analysis method of recognition-based graphical password. Jurnal Teknologi, 72(5), 2015.

[33] De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International journal of human-computer studies, 63(1-2), 128-152, 2005.

[34] Dandin, S. B., Tiwari, A., & Kaur, M. Security Analysis of Graphical Passwords Over the Textual Passwords for Authentication. International Journal of Engineering Research and Technology, 3(10), 2014.

[35] Suru, H. U., & Murano, P. Security and user interface usability of graphical authentication systems–A review. International Journal of Engineering Trends and Technology (IJERT), 67, 17-36, 2019.

[36] Khodadadi, T., Islam, A. K. M., Baharun, S., & Komaki, S. (2016). Evaluation of Recognition-Based Graphical Password Schemes in Terms of Usability and Security Attributes. International Journal of Electrical & Computer Engineering (2088-8708), 6(6), 2016.

[37] Lashkari, A. H., Farmand, S., Zakaria, D. O. B., & Saleh, D. R. Shoulder surfing attack in graphical password authentication. arXiv preprint arXiv:0912.0951, 2009.

[38] Gao, H., Liu, X., Wang, S., Liu, H., & Dai, R. (2009, December). Design and analysis of a graphical password scheme. In 2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC) (pp. 675-678). IEEE, 2009.

[39] Yang, G. C. (2020). A Multimodal Password System based on Graphics and Text. Engineering Letters, 28(2), 2020.