Graphical User Authentication Algorithms Based on Recognition: A Survey

Zena M. Saadi[1†], Ahmed T. Sadiq[1] and Omar Z. Akif[2]

[1]Department of Computer Science, University of Technology, Baghdad, Iraq

[2]Department of Computer Science, College of Education for Pure Science (Ibn al-Haitham), University of Baghdad, Baghdad, Iraq

***Abstract*—In cyber security, the most crucial subject in information security is user authentication. Robust text-based password methods may offer a certain level of protection. Unfortunately, extensive use of strong passwords is barely feasible since people who use them tend to write them on paper or store them in a computer file. Many computer systems, networks, and internet-based environments have tried adopting graphical authentication methods in the past few years for user identification. It is significant to note that security and usability are the two main attributes of all graphical passwords. Unfortunately, none of these methods can effectively solve both of these issues at the same time. The aspects of the discussion included the ISO usability standards and characteristics of graphical user authentication and possible pre-attacks on 19 recognition-based authentication systems. In the current analysis, the differentiation table of attack patterns for all recognition-based techniques is revealed. Finally, the nineteen methods' positive and negative aspects were explained in a detailed table.**

***Index Terms*—Graphical Password, Graphical User Authentication, ISO usability, Possible attacks, Recognition, Security.**

I. Introduction

Information security refers to the practices, technologies, and processes designed to protect sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes protecting information in various forms, such as electronic, physical, or verbal, from threats, vulnerabilities, and risks, Encryption is the process of converting plaintext (readable data) into unreadable ciphertext to protect it from unauthorized access. This is done using an encryption algorithm and a secret key. The utilization of alphanumeric passwords has traditionally been employed to ensure the authenticity of a user. Many people tend to remember visuals more easily than text; graphical authentication has been suggested as a potential replacement for text-based authentication (Farid, et al., 2021). Despite the availability of alternative identification techniques, such as biometrics and smart card technology in the present time, it is highly likely that the password system will remain dominant due to the concerns surrounding dependability, privacy, simplicity of use, and security associated with alternative methods (Siddiqui, et al., 2018; Latee, et al., 2023). The majority commonly used method for authenticating a user within a system is the textual password. This method is currently commonly used for user authentication in computer systems, internet-based contexts, and networks (Gao, et al., 2010; Nagothu, et al., 2019; Furkan, Ant and Stephen, 2006). However, the vulnerabilities of this approach are widely recognized. Most passwords can be easily guessed or cracked. For example, the dictionary attack is a frequently employed method for hacking into an alphanumeric password (Susan, et al., 2005). This attack is highly efficient, as it requires minimal time to uncover the user's password (Amna, Kenz and Wafa, 2021; Leon and Boštjan, 2020). Moreover, another shortcoming of this strategy is the challenge of maintaining password memory. Recent studies have demonstrated that humans have a limited capacity to remember multiple passwords (Zhao and Li, 2007; Lashkari, et al., 2011). An inherent challenge with alphanumeric passwords is that users must recall them when logging into systems where they have been employed. Nevertheless, humans frequently forget their passwords, especially if they are not used continuously. As a result, people frequently write down their passwords or choose readily guessed passwords, such as the names of their pets, close friends, or birthdays (Nicholas, Andrew and Robert, 2012). Another form of password strategy that has been proposed for many security systems is the graphical password technique. Graphical passwords are potentially simpler to recall and offer enhanced security in contrast to conventional alphanumeric passwords, as they leverage humans' ability to memorize and recall images more effectively (Erlich and Zviran, 2009).

This methodology was devised to tackle the challenges linked with traditional passwords utilizing alphanumeric

ARO-The Scientific Journal of Koya University
Vol. XII, No. 2 (2024), Article ID: ARO.11603. 15 pages
Doi: 10.14500/aro.11603
Received: 24 April 2024; Accepted: 08 August 2024
Regular review paper; Published: 23 August 2024
†Corresponding author's e-mail: cs.22.15@grad.uotechnology.edu.iq

http://dx.doi.org/10.14500/aro.11603

structures. It not only enhances memorization and user-friendliness but also offers enhanced security (Lazar, et al., 2011; Biddle, Chiasson and Oorschot, 2012). Grounded on the premise that individuals possess superior image retention abilities in comparison to numbers and words and that a single image carries more significance than multiple passwords, both software firms and behavioral scientists appear to endorse this methodology (Komanduri and Hutchings, 2008). Searchmetric or Cognometric systems, also referred to as Recognition-Based systems, necessitate users to memorize and recognize image collections when setting passwords, and subsequently (Constantine, et al., 2023), when logging in, and detecting images among distractors. Put differently, in the Recognition-Based approach, users are shown a series of images, and validation is accomplished by recollecting and picking out the designated image during the initial enrollment phase. Diverse categories of images are employed by the proposed recognition-based systems, such as symbols, abstract art, facial features, and common objects (Gao, et al., 2010).

A graphical password, also known as an image-based password or pictorial password, is a password scheme that uses an image, logo, or gesture instead of or in addition to text to verify an identity or validate authentication. However, due to the limited implementation of recognition-based graphical password systems, the vulnerabilities associated with these schemes are not yet fully comprehended. In general, the current techniques employed in recognition-based graphical passwords are still in their nascent stage. Extensive research and user studies are imperative to enhance the maturity and utility of these techniques. This study encompasses a comprehensive investigation into the existing recognition-based graphical password scheme, evaluating both its strengths and weaknesses (Komanduri and Hutchings, 2008). Moreover, it analyzes and identifies the usability characteristics and potential threats to recognition-based graphical passwords. In addition, a comprehensive and comparative evaluation of the usability attributes, attacks that occur and the pros and cons of each of the various recognition-based graphical password techniques are listed, aspects that have not received sufficient attention in prior studies (Brostoff and Sasse, 2000).

II. Schemes Based on Recognition

This section enumerates and elucidates a selection of recognition-focused frameworks that were examined from the years 2000 to 2023, emphasizing their limitations.

A. The Passface Scheme

In 2000, the Passface scheme was developed by the Real User Corporation (Brostoff and Sasse, 2000). A commercial product known as Passfaces was introduced by the Real User Corporation, based on the premise that individuals possess superior memory retention for faces as opposed to other types of images. Users of Passfaces are required to choose a human face from a collection of nine options, where only one face is recognizable to them while the rest function as distractors. This iterative process continues until all four faces are correctly identified. A comparative analysis of Passfaces passwords indicated that users exhibited greater ease in remembering Passfaces in contrast to text-based passwords. Moreover, users displayed significant susceptibility to factors such as the characteristics of the faces used, such as their ethnicity, gender, and attractiveness (Sabzevar and Stavrou, 2008). As a result, the predictability of Passfaces passwords could potentially be compromised. One potential resolution to this challenge is the random assignment of faces to users, although this approach would heighten the difficulty for users to memorize their passwords. Furthermore, the use of Passfaces for login and registration processes can be time-consuming in comparison to text-based password systems. Further studies were conducted to assess the security features of PassFaces, particularly its susceptibility to social engineering threats where hackers attempt to manipulate users into revealing their chosen image (Khan, Din and Almogren, 2023; Levin, 2000). This study revealed that if a decoy image is carefully chosen to resemble the user's selection, it is not possible for another individual to accurately enter the password solely based on the description of the image they have heard in the Fig. 1.

B. Déjà vu Scheme

This strategy, which was introduced in 2000, allows consumers to choose a predetermined number of photographs from a big portfolio. The images were created using random art, one of the hash visualization algorithms, because the designer wished to lessen the possibility of a description attack. The color value of each pixel in the image is defined by a random mathematical formula that is generated when one initial seed is provided. One random abstract image will be the result, as seen in Fig. 2. Since the image is solely dependent upon only a seed are must be kept on the trusted server; it is not required to retain the images pixel by pixel for the first seed. The user must successfully navigate a difficult sequence of photos during the authentication step, some of which are spoof images mixed in with his portfolio.

Fig. 1. Passface Scheme by Brostoff and Sasse.

The user will be verified if he or she is able to successfully select their whole portfolio (Rachna and Adrian, 2000).

There are various issues with this approach. First off, it takes the user more than 60 s to create a portfolio using this method a longer period than it takes to create a text password which is 25 s. Compared to using a text password, the login process using this method takes the user longer (Khan, Din and Almogren, 2023). However, the user may find the procedure of choosing an image from the database to be time-consuming and laborious. The requirement to save the seeds in each user's plain text portfolio image could be another disadvantage (Nagothu, et al., 2019).

C. Triangle Scheme

A group presented the Triangle algorithm in 2002, and it produced numerous techniques that can thwart a shoulder surfing attack. Triangle, their initial scheme, is depicted in Fig. 3. Using this strategy, a set of N objects that could number in the hundreds or thousands is randomly displayed on the screen by the system. A subset of K previously selected and memorized objects are also present. Stated otherwise, these K objects represent the user passwords.

The user must locate three of its password objects, then click inside the invisible triangle formed through these three objects, or click inside a convex hull of the displayed scroll objects, after a system randomly selects a placement object N after login. In addition, this task is replayed several times for each login, utilizing different displays for some N objects. As a result, there is very little chance that you will coincidentally click in the right area in each task (Sobrado and Birget, 2002).

There are various issues with this approach. To make this method resistant against shoulder surfing attacks, the method's designer recommended using one thousand objects throughout the login process. However, the use of so many objects makes the display extremely congested and the objects themselves nearly indistinguishable. On the other hand, employing fewer objects will result in a smaller password space and a larger convex hull (Nagothu, et al., 2019).

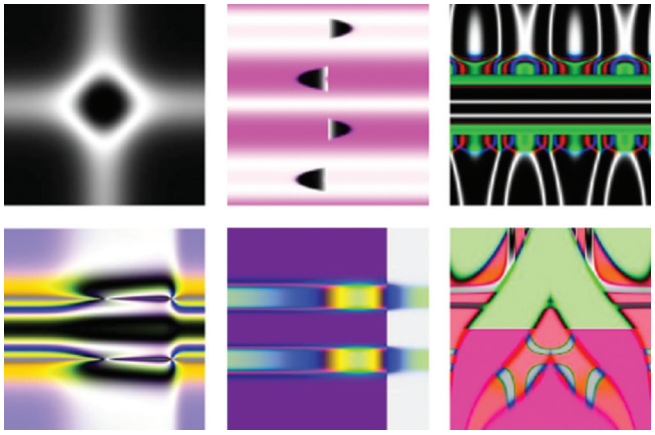

Fig. 2. Déjà vu Scheme by Rachna and Adrian.

Fig. 3. Triangle Scheme by Sobrado and Birget.

D. Movable Frame Scheme

This model was created in 2002 using the same designers and based on the same concepts and presumptions as a triangle scheme. Using this method, the user has to find three things out of K; these three objects are their passwords. As Fig. 4 illustrates, only three pass objects are ever exhibited at once, and only one of those things is ever housed in a movable frame.

To align the password object is on the frame with the other two pass objects, the user must drag the mouse around the frame and the objects inside it during the login process. The process is carried out several times to reduce the possibility of the frame being moved at random (Rachna and Adrian, 2000). Due to the excessive number of objects, this approach has the disadvantage of being a tedious, complicated, and time-consuming process, this schema has used in some applications as

1. Robotics: The scheme is used to model and control robotic arms, humanoid robots, and other complex robots.
2. Computer vision: The scheme is used to track moving objects and estimate their trajectories.
3. Biomechanics: The scheme is used to model and analyze human movement, including gait analysis and motion simulation (Furkan, Ant, and Stephen, 2006).

E. Picture Password Scheme

This algorithm was created in 2003 specifically for handheld devices such as PDAs (personal digital assistants).

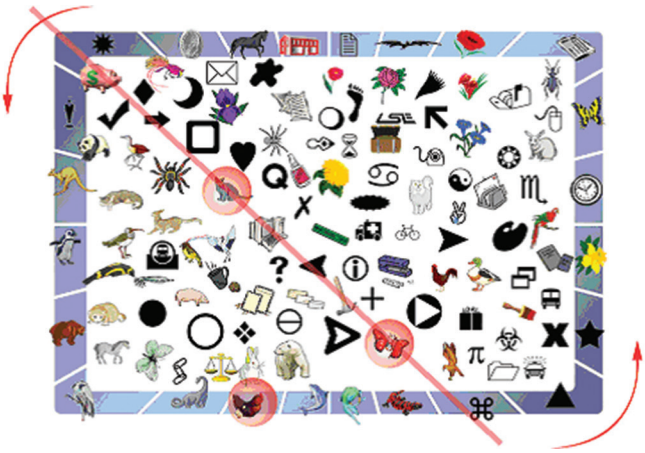

Fig. 4. Moveable Frame Scheme Furkan, Ant and Stephen.

http://dx.doi.org/10.14500/aro.11603

As illustrated in Fig. 5, a user registers a series of thumbnail images that will be used as a password in the future after choosing a theme that indicates the thumbnail photos to be applied. The user needs to enter the currently enrolled image sequence for verification on turning on the PDA to access the device. On successful authentication, the user has the option to modify their password and choose an alternative theme or sequence.

The password space is deemed small because there is a 30-photo limit on thumbnail images. Therefore, the designer included a second way to choose the thumbnail item to guarantee that a password space is equivalent to the alphanumeric. In addition to choosing individual thumbnail components as previously, it is also possible to choose two thumbnail items together to create a new alphabet item. Previously, this was accomplished by using a shift key on a conventional keyboard to pick uppercase or special letters; however, in this case, each thumbnail item acts as a shift key for all other items, including it. The password space increases from thirty to nine hundred and thirty items with this modification, which is comparable to the 95 printable ASCII characters that are accessible from a conventional keyboard. However, doing so will increase the complexity and difficulty of the generated password's memorability (Jansen, et al., 2003). This model's disadvantage is that the shift key adds complexity and difficulty to the algorithm.

F. Where is Waldo (WIW) Scheme

This algorithm was presented by Man, et al. as a technique for making graphical password shoulder surfing resistant in 2003. Every image in this algorithm has been given a distinct code. As illustrated in Fig. 6, the user is presented with multiple scenes during authentication, each containing multiple password objects and multiple decoy ones. The user will input the code string that corresponds to his password since every password object has a distinct code. Even if the complete authentication procedure is recorded; it is extremely difficult for a shoulder surfer to crack this type of password. Users still need to commit the code to memory for every password object variation when using this method, though. In the event that four photos are presented, each with four variations, the user must commit sixteen codes to memory.

The disadvantage of this approach is that it is cumbersome for the user to memorize all case-varying passwords, even though the password objects offer some clues for remembering the codes (Tu, Dahai and Yun, 2021).

G. Story Scheme

The story concept from 2004 divided the pictures that were accessible into nine categories: vehicles, women, food, animals, kids, men, objects, nature, and sports. To create an easily remembered story, users must choose their passwords from a mixed picture of nine different categories, as seen in Fig. 7. Some people employed this technique without coming up with their own narrative (Darren, Fabian, and Michael, 2004).

According to this study, remembering the story scheme was more difficult than using Passface authentication.

H. Jetafida Scheme

This approach was introduced in 2008 in an attempt to compile all the usability features such as design and layout acceptability, ease of use, ease of creation, ease of memorization, and ease of learning into a single algorithm.

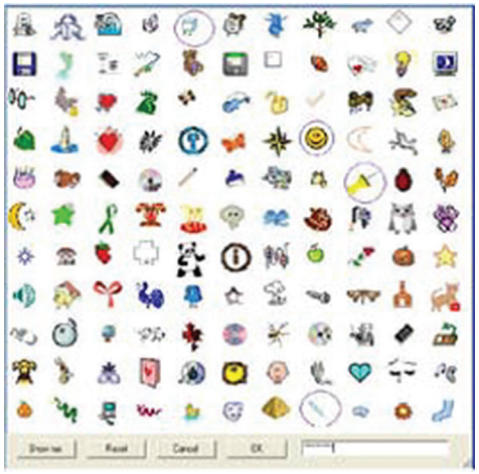

Fig. 6. Man et al. Scheme by Tu, Dahai and Yun.

Fig. 5. Picture Password Scheme by Jansen, et al.

Fig. 7. Story Scheme by Darren, Fabian, and Michael.

As illustrated in Fig. 8, the user will choose three images as a password during registration and arrange them in the order he desires during the login process.

To improve usability during the login process, the user's password will be combined with seventeen-colored graphics. Thirty or so individuals use the trial version. They stated that 53% of users thought the design and screen layout were appropriate, 40% thought the algorithm was easy to use, 50% thought it was easy to create, 55% thought the new algorithm was easy to memorize, and 57% of users agreed the algorithm is easy to learn (Ali and Norafida, 2008). Since the method is so young, no survey has yet found a unique disadvantage.

I. WYSWYE ("Where You See is What You Enter") Scheme

Khot, Kumaraguru, and Srinathan (2012) presented a secure scheme to counteract shoulder-surfing attacks in recognition-based graphical passwords (Khot, Kumaraguru and Srinathan, 2012). The technique utilized the WYSWYE scheme, as shown in Fig. 9 which requires users to select image-based password patterns from an image grid and replicate them on another grid. WYSWYE symbolizes on "Where You See (the password) is What You Enter (the position)". This scheme, based on the concept of tabular reductions and identification of patterns, is both straightforward and efficient. It involves identifying the pattern of N password images within an M×M grid and mapping them onto an independent N×N grid. During the login process, the Challenge grid is displayed next to an empty, randomly generated image grid created by the system, which consists of the M×M grid with N password pictures and M2-N decoy pictures. However, the users do not directly interact with this grid. Instead, they use a distinct N×N grid called the Response grid, which is positioned on the right-hand side of the screen, to enter their input. To successfully log in, the users need to accurately recognize the patterns of the password images and replicate them in the Response grid.

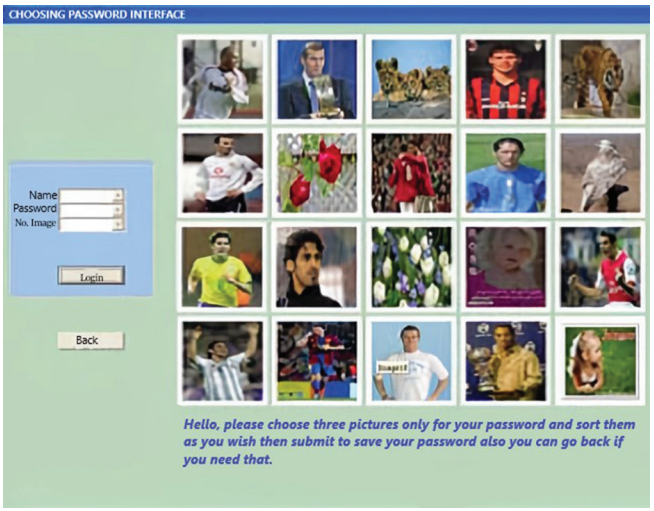

Fig. 8. Jetafida Scheme by Ali and Norafida.

J. Ho et al.'s Scheme

In 2014, Ho et al. introduced an approach (Ho, et al., 2014) that permits the challenge set's input to consist of both registered and decoy images. The user must register multiple photos during the registration process. The order of the registered photographs must be retained by the user. Using the initial picture, the cued image, and the suggested method, a pass-image is produced during the authentication process. The initial image marked at the start and the prompted image corresponds to the first and second images that have been registered, respectively. The pass-image is then obtained by applying the suggested technique. The user must decide if the

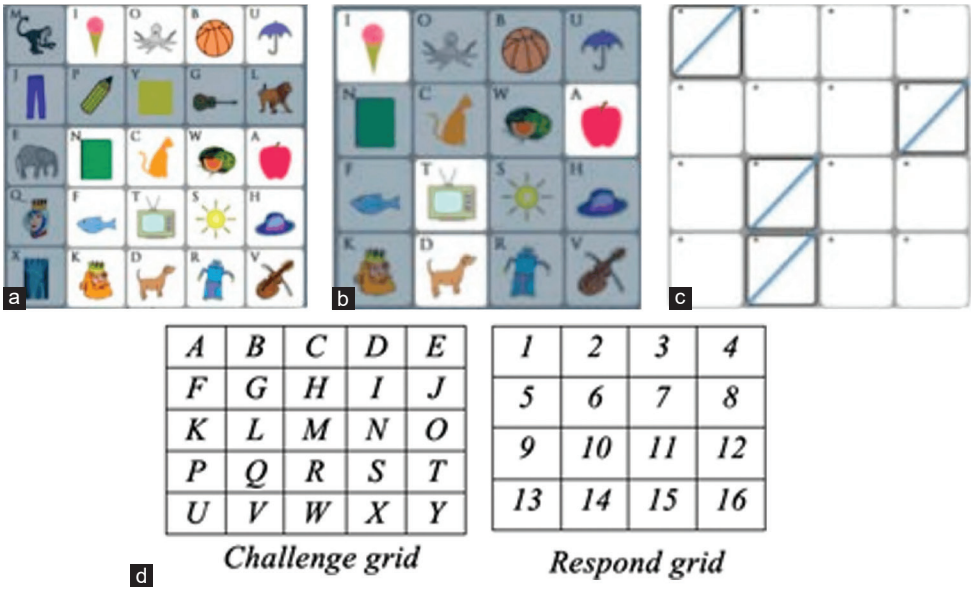

Fig. 9: Where You See is What You Enter (WYSWYE; adapted from Nagothu et al.) user interface by Khot, Kumaraguru, and Srinathan. (a) Users must mentally cross out each row and column from the challenge grid that doesn't have the password images in this example, an apple, a dog, ice cream, and television. (b) Users must determine where the password images are located in the grid with less challenge. (c) Users must click where the password images are located in the response grid. (d) Sample notations that are used in the challenge and respond grids to highlight WYSWYE's shortcomings.

http://dx.doi.org/10.14500/aro.11603

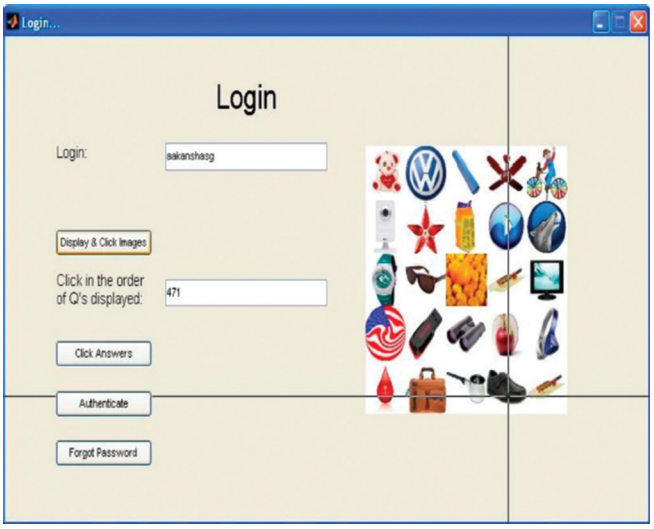

Fig. 10. The Gokhale and Waghmare system's user interface by Gokhale and Waghmare.

Fig. 11. The system's user interface by Por, et al.

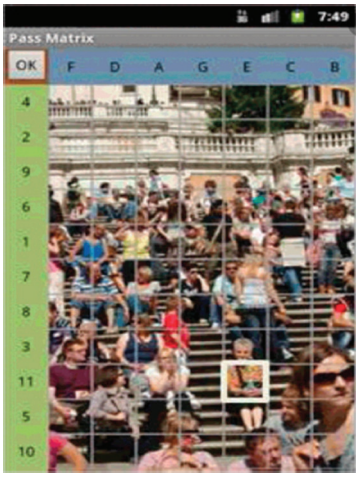

Fig. 12. The system's user interface by Sun, et al.

cued picture is on half the imaginary line in the suggested technique. The amount of offset is determined at one in the event that the cued picture is not on half the imaginary line. The pass-image is therefore the picture that follows the

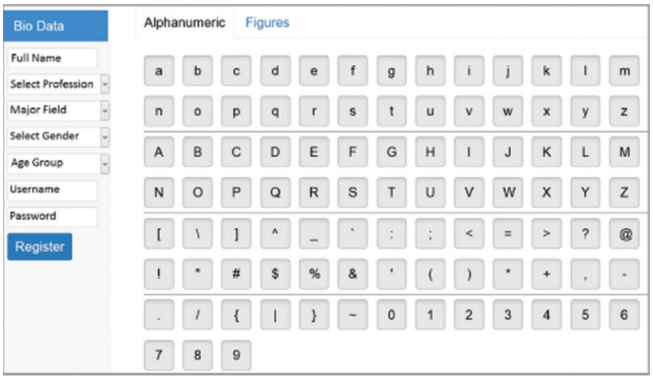

Fig. 13. Displaying an alphanumeric characters registration screen by Nizamani, Hassan, and Shaikh.

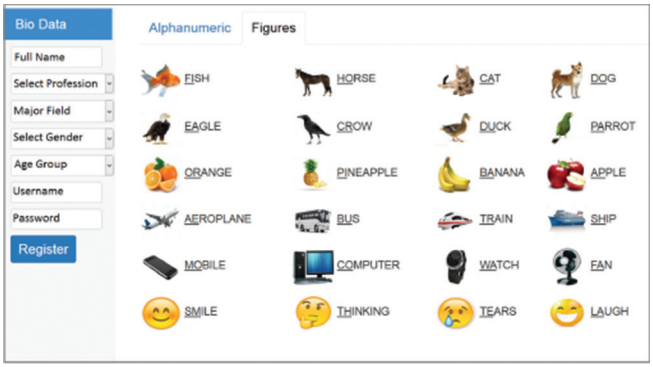

Fig. 14. Registration screen with visual representations by Nizamani, Hassan, and Shaikh.

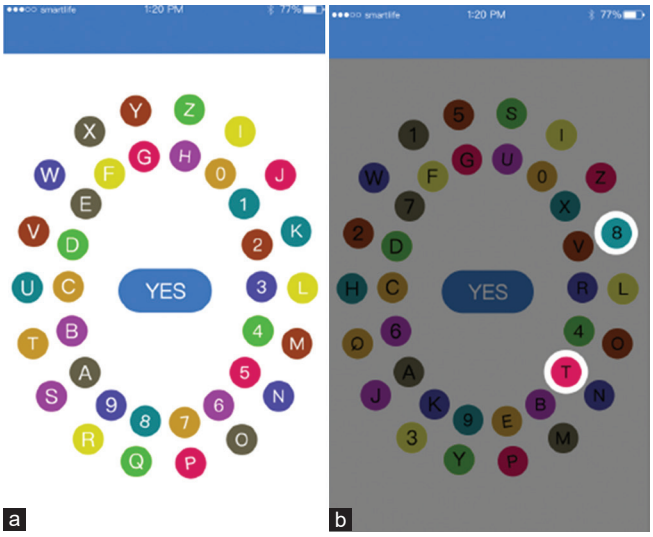

Fig. 15. The first stage of login verification by Li, et al. (a) Primary interface. (b) The system passes implicitly "8,T" as a user login indicator.

beginning image immediately along the imaginary half-line. It is necessary for the user to verify whether the cued picture is the final image on the half imaginary line if it is on it. The highest offset is used if the cued picture is not the final image on the hypothetical half-line. Consequently, the pass-image is last picture along the hypothetical half-line (Por, Ku and Ang, 2019). The quantity offset is lowered by one if the cued picture appears last on the hypothetical half-line.

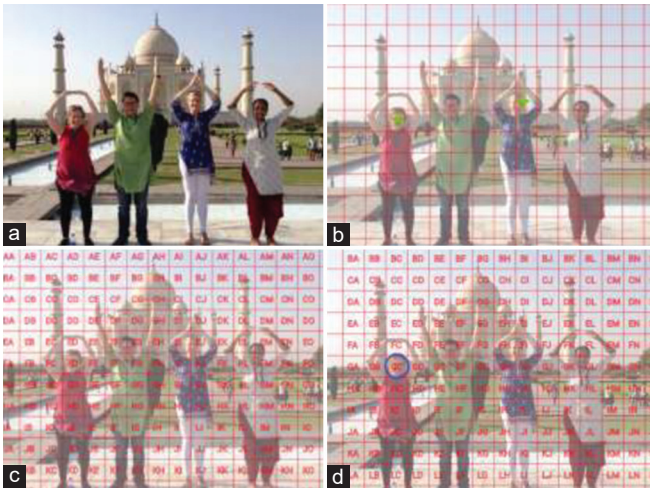

Fig. 16. Aligned over the first click point (Rajarajan and Priyadarsini). (a) User's password image. (b) Click points chosen by user indicated by circles. (c) Image presented with grid of alphabets. (d) Secret token 'GC'.

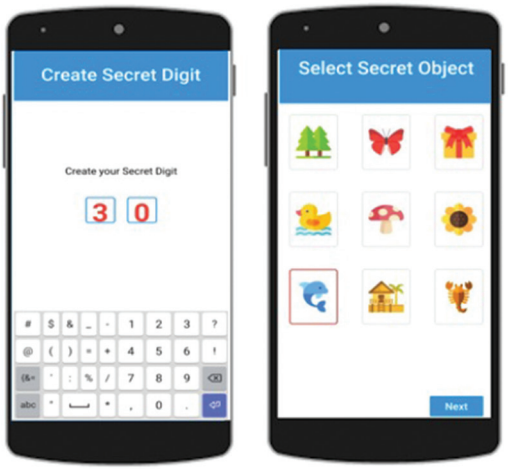

Fig. 17. Select 2-digit secret number and one secret image by Kausar, et al.

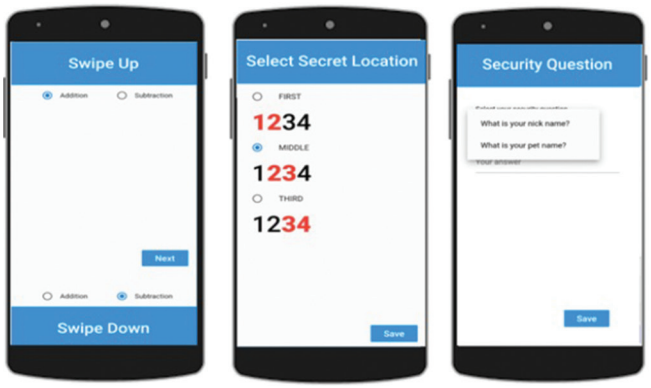

Fig. 18. Select arithmetic operation, secret position, and security question by Gao, et al.

Consequently, the pass-image is the picture that comes before the final image along the hypothetical half-line. The identical procedure is utilized to identify the next pass-image; the only differences are that the cued picture is the second registered image and the beginning image is the current pass-image.

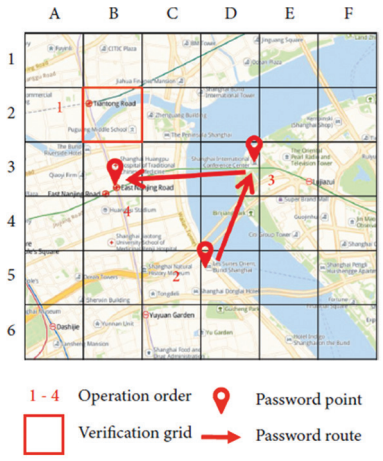

Fig. 19. Selection of verification grids and password path in registration phase.

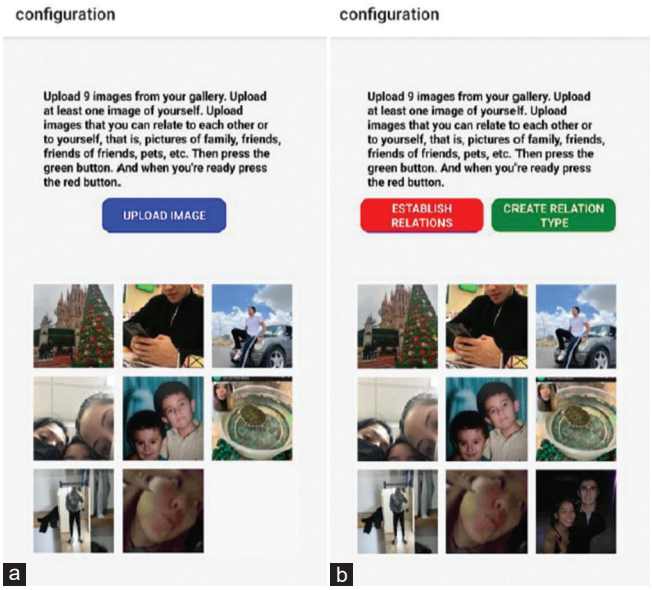

Fig. 20. Multi-Factor Authentication Scheme. (a) Image loading screen. (b) The Image upload screen once the user has uploaded nine images by Kausar, et al.

Up until the last pass-image is achieved, this procedure is repeated. The user must click the last pass-image to log in.

This technique can stop direct observation attacks, suggests (Ho, et al., 2014). Nevertheless, the system is susceptible to reverse engineering assaults when numerous sessions are videotaped (Por, Ku and Ang, 2019). Attacks using reverse engineering take advantage of the constancy of the registered photos utilized in a challenge set. One way to conduct a reverse engineering attack is to exclude certain images that are not possible to be the final cued image. By determining the final beginning image or eliminating more photos, an attacker can then get the remaining registered images. As a result, attackers can identify the registered photos and log in using those identities.

K. Gokhale and Waghmare's Scheme

A graphical password technique was presented by Gokhale and Waghmare in 2016 (Gokhale and Waghmare, 2016). A user

http://dx.doi.org/10.14500/aro.11603

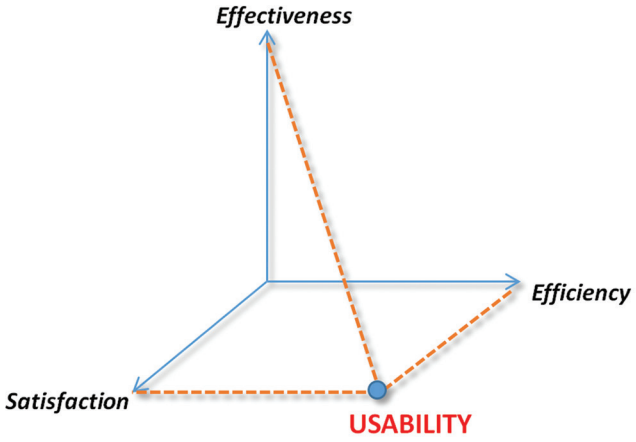

Fig. 21. The main part in IOS-9241.

must register multiple photographs from a set of 25 images during the registration process. It is required that the user register a minimum of six photographs, and the total number of images registered must be even. The order of the registered photographs must be retained by the user. The selected registered photographs are shown on a panel for the user's convenience. However, these pictures will vanish in 5 s. The user must then select a question from the pool of questions. There is a number assigned to each question. The user is needed to enter a place as the response to the question after choosing it. To help the user remember the chosen place, the user has the option to pick one of the 25 backdrop images provided by the system or upload their own image from local storage. Three locations must be registered by the user, and each place needs to be connected to a question. The user must use the registered photos to get multiple pass-images during the authentication process. Row information from the first registered image and column information from the second registered image are utilized to calculate the position of the first pass-image. The first pass-image is the intersection image. For every pair of registered photos, this procedure is repeated. Subsequently, the three sets of recorded questions are shown to the user at random. During registration, the user must click on the places linked to the questions to respond to them as shown in Fig. 10.

This technique is simple to implement and can stop shoulder-surfing attacks, claims (Gokhale and Waghmare, 2016). Attackers can readily shoulder-surf the clicked spots, though, because the locations are set (Islam, Por and Othman, 2019). In addition, after making several observations, the attackers can remove the registered photographs. This indicates that shoulder-surfing assaults can still be made against this scheme.

L. Por et al.'s scheme

A technique utilizing digraph substitution rules was presented by Por, et al. (2017). The user must register two photos throughout the registration process. After that, to log in using the first or second pass-image, the user must register. The user must choose a pass-image during authentication to log in utilizing digraph substitution rules as shown in Fig. 11.

This strategy can stop shoulder-surfing attacks, according to Por, et al. (2017). Nonetheless, through numerous shoulder-surfer sessions, attackers can simply track the clicked photos and gather details regarding the registered images provided they are aware of the underlying technique (Khot, Kumaraguru and Srinathan, 2012).

M. Sun et al.'s scheme

In 2018 (Sun, et al., 2018), Sun et al. presented PassMatrix, which makes advantage of the picture discretization algorithm, as shown in Fig. 12. The registration process requires the user to choose many photos. Every choice has a corresponding letter on the horizontal bar and a corresponding number on the vertical bar. For every pre-selected puzzle, the user must move the letter to the column on the horizontal bar and the number to the row on the vertical bar. This procedure is iterated for every chosen image. The first chosen image's random problems are then displayed. Every problem has a number at the vertical bar and a letter at the horizontal bar. For every pre-selected puzzle, the user must move the letter to the column on the horizontal bar and the number to the row on the vertical bar. Each chosen image undergoes this process once more.

This technique is capable of thwarting shoulder-surfing attacks, as per (Ho, et al., 2014). The fact that the problems and the chosen photos are fixed, however, leads us to conclude that this system is still susceptible to shoulder-surfing attacks. After several observations, an attacker may shoulder-surf the selected in advance puzzle in each of the chosen images to log in.

N. A Hybrid Textual-Graphical Authentication Scheme

In 2021, S. Z. Nizamani et al. introduced a hybrid authentication system that incorporates both text and graphic elements. This scheme encompasses a multitude of mechanisms to address the shortcomings of current security schemes. Both easy login and secure login represent two different types of password inputs that can be dynamically chosen within this framework. The primary goal of the methodologies used in this study is to create a harmonious balance between data protection and ensuring user convenience. Moreover, the framework includes a unique graphical style for password creation, which enhances memorability. Furthermore, it integrates a multi-step verification process that focuses on the idea of one-time passwords (OTPs). Furthermore, this approach takes advantage of basic arithmetic operations to enhance security measures and assigns random numerical values to password components, organizing them in a randomized order (Nizamani, et al., 2021) as shown in the Fig. 13 and 14.

The efficiency of this framework was evaluated through its implementation and evaluation of its security flexibility against various cyber threats, in addition to its ease of use and ease of retrieval. Therefore, a comparison was made between the reliability and authentication speed of this approach and eight other authentication mechanisms (Nizamani, et al., 2021).

O. PinWheel Scheme

In 2021, PinWheel was presented by Li et al. as a login authentication system. This system combines graphical passwords with biometrics. In Fig. 15. each login using this new

technique accompanies a unique challenge value that has been derived from the fixed bead chosen by the user at registration. To achieve a secure authentication, legitimate users have to enter this challenge value into the specific field to authenticate their identity. Developers can mitigate some types of attacks, such as shoulder-surfing, smudge attacks, and video analysis, by merging a local password with a text password. This effectively prevents unauthorized access to the user credentials. Furthermore, restricting login permeation for achieving reliable administrators, PinWheel combined an optional user feature-based authentication approach, for this end, improving the security of the device and protecting data privacy over an additional security layer.

PinWheel underwent rigorous testing against various attack scenarios to evaluate its security efficacy. The outcomes of these assessments were affirmative, signaling the resilience of the system. Furthermore, an extensive user evaluation of PinWheel was executed, gathering insights on long-term password retention and authentication duration from individuals who tested a trial version of PinWheel on their mobile devices. A questionnaire was formulated to facilitate data collection in the latter phases of the trial. The findings of the investigation underscored the remarkable user-friendliness of PinWheel (Li, et al., 2021).

P. SelfiePass Scheme

The SelfiePass scheme, proposed by Rajarajan et al. in 2021, presents a remedy for the susceptibility of graphical passwords in the presence of shoulder surfing threats. By allowing users to input click points on images without direct contact with the image cells, the scheme employs a grid consisting of permutations of two alphabets, accompanied by a secret token transmitted through headphones to guide users in selecting the click points as shown in Fig. 16.

During the process, the user manipulates the grid columns horizontally and vertically to position the secret token (password) on the designated column for the first click point. The system then determines the click point based on the token's placement. This procedure is repeated for the entry of the second click point, ensuring that even if an attacker records a video of the authentication process, they are unable to ascertain the actual click points. In this manner, SelfiePass establishes a secure and resilient graphical password scheme for user authentication (Rajarajan and Priyadarsini, 2021).

Q. GRA-PIN scheme

In 2022, Kausar et al. presented a hybrid authentication approach for Smart Devices. This approach combines text and graphical-based techniques, requiring users to determine four distinct options to generate a password. The four selections of GRA-PIN consist of choose of two-digit numbers, choose one secret image, choose the swipe-up/down position for arithmetic operation, and finally, choose the password position in the final four-digit PIN. In addition, the user is required to provide a secret answer in the event of forgetting the password as shown in Figs. 17 and 18. To enhance security against shoulder surfing, guessing, and camera attacks, a new password is generated each time the user logs in. Overall, this authentication technique offers enhanced reliability, security, and user-friendliness, all while maintaining usability and security (Kausar, et al., 2022).

R. VGMSGP Scheme

In 2022, Wang, et al. introduced a graphical password scheme as shown in Fig. 19 that amalgamates a verification grid and map slipping strategy to enhance the security and usability of the authentication process. During the authentication process, the user is mandated to manipulate the map to align every point on the password path within the predetermined verification grid. This particular approach thwarts shoulder-surfing attempts by complicating the task for malicious individuals in pinpointing the exact verification grid selected by the user. Across integrating the password pathway with the verification grid and employing the technique of map slipping, the system enhances the security of the authentication procedure and boosts the effectiveness of protecting against shoulder-surfing attacks by a range of 37% to 56%. In addition, the utilization of the map slipping technique enhances the user-friendliness of passwords in the system, increasing it by 3% to 6%.

In addition, using a map slipping strategy, combined with representing password points as coordinates on the map, helps reduce the storage burden of the system. This scheme successfully achieves a harmonious balance between usability and security by incorporating a map-slipping strategy as a defense mechanism against shoulder-surfing attacks (Wang, et al., 2022).

S. Multi-Factor Authentication (MFA) Scheme

In the year 2023, Carrillo-Torres et al. put forward an innovative MFA mechanism as shown in Fig. 20 that relies on image recognition and user-established connections, thus eliminating the need for supplementary hardware and ensuring simplicity of use. The integration of textual and graphical elements within the suggested mechanism increases the password space, rendering it more resilient and impervious to security threats.

The process of authentication entails users discerning specific images from a collection of randomly chosen images and establishing a self-pre-configured relationship between two specific images. A functional model of the suggested system was developed and deployed, and it underwent testing by users from various backgrounds. The algorithm underwent testing on users through the utilization of a mobile application available on both the Android and iOS platforms. The suggested system demonstrated a 100% accuracy rate in identifying and authenticating users, provided that authentication items and credentials have not been forgotten, and was discovered to be user-friendly and preferable to common MFA mechanisms (Carrillo-Torres, et al., 2023).

III. ISO Standard Usability

The biggest developer and publisher of international standards globally is the International Organization for

Standardization or ISO for short. As the ISO worked on developing methods for usability evaluation, it defined several models; however, none of these models was suitable for evaluating all the schemes. All the ISO techniques provide information on the method, its features and usability only in several cases. In this section, we shall be discussing about ISO 9241. The main part of IOS 9241 is the HERE (Human Ergonomics Requirements in Environment) part that Fig. 21. describes the user and environment requirements. (Ali and Norafida, 2008):

- *Effectiveness*: Describes the transactional level that entails how users engage with a process to achieve predetermined goals with great accuracy and detail. In other words, how effective the users are in using the system to complete the tasks meant to accomplish the laid down objectives.
- *Efficiency*: is the ratio of resources used to the accuracy and thoroughness with which users accomplish their objectives.
- *Satisfaction*: The absence of discomfort and favorable perspectives toward the product's usage. Speaks of a user's perspective or their feelings regarding the system they are using such as (Use the mouse or Pen simply, Some of the GUI qualities include: Easy generation of password, clear steps of registration and login, and attractive layout, among others (Muhammad, et al., 2015). Thus, Table I shows the comparative usability of the graphical schemes used above methods was attained.

Table I collected all of the effectiveness, efficiency, and satisfaction usability attributes. Then, the characteristics of each one of them are created based on previous research. For example, using the mouse makes the user more satisfied compared to using the keyboard. Thus, it turned out that the methods mentioned 1, 2, 3, 4, and 19 received the property of effectiveness but did not receive efficiency. It was also not pointed out that the researcher actually employs it in real-life situations. In regards to methods 13, 14, 15, 16, and 17, they managed to satisfy the effectiveness characteristic, furthermore, they are utilized in the real world with a different satisfaction characteristic.

IV. Possible Vulnerabilities in Systems for Graphical Passwords Based on Recognition

In the subsequent section, an extensive investigation into the potential assaults on recognition-based graphical password methods has been carried out and the assaults have been recognized and ascertained. The potential assaults have been correlated to the recognition-based schemes. The potential assaults have been categorized into four types of assaults, spyware, guessing, shoulder surfing, and SQL injection. These represent the current active assaults on recognition-based schemes (Khodadadi, et al., 2016; Xiaoyuan, Ying and Scott, 2005).

- *Spyware attack*
  This is a specific type of attack where sensitive data are first recorded on the user's machine through the installation of software tools. The malware records every key or mouse movement, unbeknownst to the user, and then transmits the recorded data outside of the computer. However, it is generally not possible to use key listening spyware or key logging alone to crack graphical passwords, as the effectiveness of mouse spyware in this regard has not been proven. Even if mouse tracking is successfully captured, it is insufficient to discover and crack the graphical password. Further information, including window size and position, as well as timing information, is required to fully exploit this specific threat.
- *Guessing attack*
  Users typically determine their passwords based on personal information such as the names of their pets, passport numbers, and last names. In response, hackers employ password guessing techniques to attempt to deduce passwords by trying out various possibilities. Password guessing attacks can be sorted into two primary forms: offline dictionary attacks and online password guessing attacks. In an offline dictionary attack, the attacker widely looks up the password by manipulating the inputs using one or more oracles tools. On the other hand, in an online password guessing attack, the attacker attempts an already guessed password by manipulating the inputs using one or more oracles tools. However, it seems that even graphical passwords can be easily guessed, similar to textual passwords.
- *Shoulder surfing attack*
  Shoulder surfing is the practice of attackers discovering users' credentials by either direct observation or external recording using video cameras while the actual user computes the information. Shoulder-surfing becomes extremely dangerous when attackers are able to pinpoint the precise location of users and make use of surveillance equipment and high-resolution cameras with telescopic lenses. While this poses a greater risk in a private setting, it is especially problematic in a public one. Most graphical passwords are susceptible to shoulder surfing, much like text passwords. There are now just a few recognition-based methods available to address the problem of shoulder-surfing. Table II demonstrates the comparative schemes based on recognition, in response to prevalent attacks.

As we can see in this table three schemes named, Ho et al.'s, Gokhale and Waghmare and PassMatrix do bad provide resistance against spyware attacks, guessing attacks, and shoulder surfing. For Por et al., A Hybrid Textual-Graphical Authentication and GRA-PIN provide resistance against spyware attacks in a good level, guessing attacks, and shoulder surfing. However, each method in the above table is not against SQL inject attack, for any attacker can enter the database and steal all information as passwords that must in future work design approach against this. In Table III, the most important positive and negative aspects of the mentioned recognition-based methods will be reviewed (Adebimpe, et al., 2023).

TABLE I
THE USABILITY FEATURES IN RECOGNITIONBASED SCHEMES

Ref	Recognition-Based Schemes	Usability Features										
		Satisfaction									Efficiency	Effectiveness
		Use the mouse or Pen simply	Simple Way to Create Password	Memorability	Simple Steps of Registration and Login	Esthetically pleasant Design	Easy to Understand	Easy to Implement and Deployment	Server and Browser Compatible	Change the User Interface according to the device	Easy to Correct	The Utilization in Real World	Reliability and Accuracy
1.	Passface Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
2.	Déjà vu Scheme	Yes	Yes	No	Yes	No	Yes	No	No	No	Yes	No	Yes
3.	Triangle Scheme	Yes	Yes	Yes	Yes	No	No	Yes	No	No	Yes	No	Yes
4.	Movable Frame Scheme	Yes	Yes	Yes	Yes	No	No	Yes	No	No	Yes	No	Yes
5.	Picture Password Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No
6.	Where is Waldo (WIW) Scheme	No	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes	No
7.	Story Scheme	Yes	Yes	Yes	Yes	No	Yes	No	No	No	Yes	Yes	No
8.	Jetafida Scheme	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No
9.	WYSWYE Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	No
10.	Ho et al.'s Scheme	No	Yes	Yes	No	No	No	No	No	No	No	No	No
11.	Gokhale and Waghmare Scheme	No	Yes	No	No	No	Yes	No	No	No	No	No	No
12.	Por et al. Scheme	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No
13.	PassMatrix Scheme	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes
14.	A Hybrid Textual-Graphical Authentication Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes
15.	PinWheel Scheme	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes
16.	SelfiePass Scheme	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
17.	GRA-PIN Scheme	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes
18.	VGMSGP Scheme	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
19.	Multi-Factor Authentication (MFA) Scheme	No	Yes	No	No	No	No	Yes	No	No	No	No	Yes

The "Yes" word refers to a present feature of an approach in these references while the "No" word means that the technique is not mentioned in the provided in these references

TABLE II
The Attacks on Recognition _Based Schemes

Ref	Recognition _Based Schemes	Spyware Attack	Guessing Attack	Shoulder Surfing Attack	SQL injection
1.	Passface Scheme	Bad	Good	Good	Bad
2.	Déjà vu Scheme	Bad	V.Good	V.Good	Bad
3.	Triangle Scheme	Bad	Good	Bad	Bad
4.	Movable Frame Scheme	Bad	V.Good	Bad	Bad
5.	Picture Password Scheme	Bad	Good	V.Good	Bad
6.	Where is Waldo (WIW) Scheme	V.Good	Bad	Bad	Bad
7.	Story Scheme	Bad	Good	Bad	Bad
8.	Jetafida Scheme	Bad	Bad	V.Good	Bad
9.	WYSWYE Scheme	V.Good	Bad	V.Good	Bad
10.	Ho et al.'s scheme	Bad	Bad	Bad	Bad
11.	Gokhale and Waghmare scheme	Bad	Bad	Bad	Bad
12.	Por et al. scheme	Good	Good	V.Good	Bad
13.	PassMatrix scheme	Bad	Bad	Bad	Bad
14.	A Hybrid Textual-Graphical Authentication Scheme	V.Good	Good	Good	Bad
15.	PinWheel scheme	Bad	V.Good	V.Good	Bad
16.	SelfiePass scheme	Bad	Good	Good	Bad
17.	GRA-PIN scheme	V.Good	Good	Good	Bad
18.	VGMSGP scheme	Bad	Bad	V.Good	Bad
19.	Multi-factor authentication (MFA) scheme	V.Good	V.Good	Bad	Bad

The "V.Good, Good" word refers to resistance to attack while the "Bad" word means that the technique is non-resistance to attacks

TABLE III
A Summary of the Strengths and Weaknesses of the Chosen Recognition-Based Schemes

Ref.	Author	Methodology	Positive aspects	Negative aspects	Year
1.	Brostoff and Sasse	Passface Scheme	Easy to use, create and recognize	Because this system uses a keyboard or mouse to navigate across multiple faces, it may be vulnerable to guessing and shoulder surfing attacks	2000
2.	Rachna and Adrian	Déjà vu Scheme	Reduce the chance of description attack	During the login process, choosing an image from the database can be time-consuming and laborious for the user	2000
3.	Sobrado and Birget	Triangle Scheme	Can overcome shoulder surfing attacks	Using this amount of objects makes the screen very crowded and the objects almost indistinguishable	2002
4.	Sobrado and Birget	Movable Frame Scheme	Provides an additional layer of security, offers a unique and visually appealing authentication method	Unpleasant, confusing, and time-consuming	2002
5.	Bye Janesen	Picture Password Scheme	Suitable for handheld devices such as a Personal Digital Assistant (PDA)	Little password area because there are only thirty total images	2003
6.	Man, et al.	Where is Waldo (WIW) Scheme	Shoulder surfing resistant.	The user finds it difficult to remember all of the passwords in their various instances	2003
7.	Davis, Monrose and Reiter	Story Scheme	Easy to remember	More complex to remember in comparison to Passface authentication	2004
8.	Ali Mohamed and Norafida	Jetafida Scheme	Ease of use, create, Memorize and learn	Users may face additional difficulties in recalling and replicating their selected graphical passwords	2008
9.	Khot, Kumaraguru and Srinathan	WYSWYE Scheme	Possessed higher login success rates than typical unprotected recognition-based graphical passwords, with no authentication failures, and were much more secure against shoulder surfing	Still susceptible to shoulder-surfing attacks since, after several observations, attackers can filter out the bogus pictures and log in as authentic users	2012
10.	Ho et al.	Ho et al.'s Scheme	Preventing the recurrence of analysis attacks	Because the recorded images used in the challenge set stay consistent, the system is susceptible to reverse engineering assaults when numerous sessions are video-recorded	2014
11.	Gokhale and Waghmare	Gokhale and Waghmare Scheme	It can prevent shoulder-surfing attacks and is easy to put into practice	Prone to repeated observations of attacks involving shoulder surfing (MOSSAs)	2016
12.	Por et al.	Por et al. Scheme	SSAs can be mitigated without compromising the strength of the password	Not strong enough to withstand multi-session observational attacks	2017

(Contd...)

TABLE III
(Continued)

Ref.	Author	Methodology	Positive aspects	Negative aspects	Year
13.	Sun et al.	PassMatrix scheme.	To lessen the impact of the direct observation assault, use the login indication	Tolerant of potential compromises including numerous observations and video recording	2018
14.	Nizamani et al.	A Hybrid Textual-Graphical Authentication Scheme	Provides better usability, its security against seven different security attacks	A High number of steps may affect the ease of use of the scheme, including login time Not be suitable for all users and may not improve security in all scenarios	2021
15.	Li et al.	PinWheel scheme	Prevent shoulder-surfing attacks, smudge attacks, or video analysis attacks PinWheel has good usability	Requires additional device support for the login authentication process, which limits its usability Limitations in terms of convenience and user satisfaction	2021
16.	Rajarajan and Priyadarsini	SelfiePass scheme	Resistant to shoulder surfing attacks Enhancing usability	The sources do not explicitly mention any vulnerability in the SelfiePass scheme	2021
17.	Kausar, et al.	GRA-PIN scheme	It is more reliable, robust, and user-friendly for smart devices Resistant for shoulder surfing, guessing, and camera attacks	The sources do not explicitly mention any vulnerability in the GRA-PIN scheme but many future trends can enhance the security: for example, using a touch or fingerprint sensor, GPS, microphone, etc.,	2022
18.	Wang et al.	VGMSGP scheme	Can effectively defend against shoulder-surfing attacks and reasonable usability simultaneously The use of Google Maps API helps to reduce the storage pressure of the system in a networked environment	Not resistant the strong shoulder-surfing attacks, i.e., multiple camera recordings while users are logged in	2022
19.	Carrillo-Torres et al.	Multi-factor authentication (MFA) scheme	Not require additional hardware, making it cost-effective and easy to implement Easy to use and preferable over common MFA mechanisms	It may still face usability challenges in terms of user acceptance and ease of use There may be failed authentication attempts because the user forgets the relationships between images	2023

V. Discussion

This investigation has brought to light the fact that various proposed graphical authentication schemes based on recognition have both advantages and disadvantages. It is not surprising that the majority of these schemes are intended to be memorable, as the primary objective of graphical passwords is to relieve the cognitive burden associated with textual passwords. The relationship between usability and security is commonly perceived as a trade-off, where enhancing one aspect tends to have a corresponding impact on the other.

Effective and safe graphical password schemes allow for passwords that are both easy to remember and complex enough to withstand attacks such as shoulder-surfing and spyware attacks. The procedure for logging in must be uncomplicated and efficient, as it is the most ordinary task performed by users of authentication systems. Our inquiry has proven this; memorability is a critical factor in login performance since it is the primary predictor of successful logins. The problem of remembering passwords over varying lengths of time and with varying login frequencies is addressed by memorability measures. While increasing memorability has been the main focus of research on graphical passwords, new usability issues have also surfaced. For example, it typically takes longer to authenticate using these methods. Users often complain that the procedure for logging in and creating a password are time-consuming, specifically when using recognition-based approaches. During registration, for instance, users must select pictures from a range of options.

In adopting the use of pass-images, during the authentication, users are required to scan through many pictures in a process that might turn out to be tiresome. Moreover, it is established that most users are ignorant about the graphical passwords and therefore, are not as flexible as the text passwords. Since text-based passwords are smaller in size as compared to graphical passwords, there is a clear indication that a lot of images are required to be stored within one database. The network transfer delay is another problem; this is mainly due to recognition-based techniques, which require the display of numerous images at every verification phase. The observed case on current schemes of visual passwords does not involve password modification or reset even though there is usually a requirement for such procedures when a password cannot be remembered.

VI. Conclusion and Future Research

This study has examined nineteen contemporary recognition-based graphical password systems. The security and usability characteristics of these systems have been further analyzed and discussed in depth. Subsequently, comparative tables of algorithms based on recognition were constructed, focusing on usability aspects and potential security attacks. Ultimately,

it was observed that since the inception of graphical image authentication methods, researchers have continuously strived to introduce novel techniques or enhance existing ones, particularly aiming at improving usability and security. Regrettably, efforts to enhance usability often lead to a reduction in security measures, while prioritizing security compromises usability features. Table II highlights that numerous recognition-based graphical password protocols, believed to be resilient against common attacks, such as shoulder-surfing, exhibit notable usability limitations, particularly in terms of prolonged login times, high success rates required for authentication, and issues with memorability, rendering them less practical for daily use. It is considered one of the most important types of attacks, SQL injection and the design of any model must be taken into account to avoid the attack and data theft, this challenge is particularly evident in recognition-based graphical password systems, where users are tasked with selecting specific images visible on the screen. Consequently, the design community faces the ongoing challenge of devising a method that effectively balances security and usability. Further research is warranted to substantiate the claim that individuals are more adept at remembering graphical passwords than textual ones, as existing user studies are scarce and inconclusive in supporting this assertion. Emphasizing the usability perspective, it is imperative to investigate the impact of using specific images as graphical passwords, assess the efficiency of proficient users, and identify common insecure practices users employ when creating graphical passwords.

References

Adebimpe, L.A., Ng, I.O., Idris, M.Y.I., Okmi, M., Ku, C.S., Ang, T.F., and Por, L.Y., 2023. Systemic literature review of recognition-based authentication method resistivity to shoulder-surfing attacks. *Applied Sciences*, 13, p.10040.

Ali Mohamed, E., and Norafida, I., 2008. Graphical Password: Prototype Usability survey. In: *International Conference on Advanced Computer Theory and Engineering*, pp.351-355.

Ali, M.E., and Norafida, I., 2008. Graphical password: Comprehensive study of the usability features of the recognition base graphical password methods. In: *3rd International Conference on Convergence and Hybrid Information Technology*, pp.1137-1143.

Amna, J.A., Kenz, A.B., and Wafa, I.E., 2021. Develop Graphical Passwords Authentication System Resistant To Shoulder Surfing Attacks. In: The 7th *International Conference on Engineering and MIS 2021* (*ICEMIS'21*). Association for Computing Machinery, New York, USA, p.55.

Biddle, R., Chiasson, S., and Oorschot, P., 2012. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys* (*CSUR*), 44, pp.1-41.

Brostoff, S., and Sasse, M.A., 2000. Are passfaces more usable than passwords? A field trial investigation. In: McDonald, S., Waern, Y., and Cockton, G., (eds) *People and Computers XIV - Usability*. Springer, London.

Carrillo-Torres, D., Pérez-Díaz, J.A., Cantoral-Ceballos, J.A., and Vargas-Rosales, C., 2023. A novel multi-factor authentication algorithm based on image recognition and user established relations. *Applied Sciences*, 13, p.1374.

Constantine, S., Margherita, A., Stavroula, N., and Gavriel, S., 2023. HCI International 2023 Posters. In: *25th International Conference on Human-Computer Interaction, HCII, Copenhagen, Denmark, July 23-28, Proceedings, Part IV. Communications in Computer and Information Science*. Vol. 1835, Springer, Cham.

Davis, D, Monrose, F., and Reiter, M.K., 2004. On User Choice in Graphical Password Schemes. In: *Proceedings of the 13th USENIX Security Symposium*.

Erlich, Z., and Zviran, M., 2009. Authentication methods for computer systems security. In: *Encyclopedia of Information Science and Technology.* 2nd ed., Vol. 1. IGI Global, United States, pp.288-293.

Farid, B., Mat, M.L., Lip, Y., and Zaidan, A.A., 2021. A systematic review of PIN-entry methods resistant to shoulder-surfing attack. *Computers and Security*, 101, p.102116.

Furkan, T., Ant, O., and Stephen, H., 2006. A Comparison of Perceived and Real Shoulder-Surfing Risks between Alphanumeric and Graphical Passwords. In: *Proceedings of the Second Symposium on Usable Privacy and Security* (*SOUPS '06*). Association for Computing Machinery, New York, USA, pp.56-66.

Furkan, T., Ant, O., and Stephen, H., 2006. *Symposium on Usable Privacy and Security* (*SOUPS*). Pittsburgh, PA, USA, pp.56-66.

Gao, H., Ren, Z., Chang, X., Liu, X., and Aickelin, U., 2010. A New Graphical Password Scheme Resistant to Shoulder-Surfing. In: *Proceedings International Conference on Cyberworlds*, CW Network, United States.

Gao, H., Xiyang, L., Wang, S., Liu, H., and Dai, R., 2010. Design and Analysis of a Graphical Password Scheme. In: *2009 4th International Conference on Innovative Computing, Information and Control*, (*ICICIC*), pp.675-678.

Gokhale, M., and Waghmare, V., 2016. The shoulder surfing resistant graphical password authentication technique. *Procedia Computer Science*, 79, pp.875-884.

Ho, P.F., Kam, Y.H.S., Wee, M.C., Chong, Y.N., and Por, L.Y., 2014. Preventing shoulder-surfing attack with the concept of concealing the password objects' information. *ScientificWorldJournal*, 2014, p.838623.

Islam, A., Por, L., and Othman, F., 2019. A review on recognition-based graphical password techniques. In: *Computational Science and Technology, Lecture Notes in Electrical Engineering*. Springer, Singapore.

Jansen, W., Gavrila, S., Korolev, V., Ayers, R., and Swanstrom, R., 2003. *Picture Password: A Visual Login Technique for Mobile Devices.* National Institute of Standards and Technology, Gaithersburg, MD.

Kausar, N., Din, I.U., Khan, M.A., Almogren, A., and Kim, B.S., 2022. GRA-PIN: A graphical and PIN-based hybrid authentication approach for smart devices. *Sensors* (*Basel*), 22, p.1349.

Khan, M.A., Din, I.U., and Almogren, A., 2023. Securing access to internet of medical things using a graphical-password-based user authentication scheme. *Sustainability*, 15, p.5207.

Khodadadi, T., Muzahidul Islam, A.K.M., Baharun, S., and Komaki, S., 2016. Evaluation of recognition-based graphical password schemes in terms of usability and security attributes. *International Journal of Electrical and Computer Engineering*, 6, pp.2939-2948.

Khot, R.A., Kumaraguru, P., and Srinathan, K., 2012. WYSWYE: Shoulder Surfing Defense for Recognition based Graphical Passwords. In: *Proceedings of the 24th Australian Computer-Human Interaction Conference*, pp.285-294.

Komanduri, S., and Hutchings, D., 2008. Order and Entropy in Picture Passwords. In: *Proceedings - Graphics Interface*, pp.115-122.

Lashkari, A.H., Abdul Manaf, A., Masrom, M., and Daud, S.M., 2011. Security evaluation for graphical password. In: Cherifi, H., Zain, J.M., and El-Qawasmeh, E., (eds) *Digital Information and Communication Technology and Its Applications: Communications in Computer and Information Science*. Vol. 166. Springer, Berlin, Heidelberg.

Latee, F., Ian, O., Mohd, Y., Mohammed, O., Chin, S., and Tan, F., 2023. Systemic literature review of recognition-based authentication method resistivity to shoulder-surfing attacks. *Applied Sciences*, 13(18), p.10040.

Lazar, L., Tikolsky, O., Glezer, C., and Zviran, M., 2011. Personalized cognitive passwords: An exploratory assessment. *Information Management and Computer Security*, 19, pp.25-41.

Leon, B., and Boštjan, B., 2020. Shoulder surfing experiments: A systematic literature review. *Computers and Security*, 99, p.102023.

Levin, D.T., 2000. Race as a visual feature: Using visual search and perceptual discrimination tasks to understand face categories and the cross-race recognition. *Journal of Experimental Psychology: General*, 129, pp.559-74.

Li, Y., Yun, X., Fang, L., and Ge, C., 2021. An efficient login authentication system against multiple attacks in mobile devices. *Symmetry*, 13, p.125.

Muhammad, D., Abdul, H., Norafida, I., and Hazinah, K., 2015. Towards Identifying Usability and Security Features of Graphical Password in Knowledge based Authentication Technique. In: *Second Asia International Conference on Modeling and Simulation*, pp.396-403.

Nagothu, D., Chen, Y., Blasch, E., Aved, A., and Zhu, S., 2019. Detecting malicious false frame injection attacks on surveillance systems at the edge using electrical network frequency signals. *Sensors* (*Basel*), 19, p.2424.

Nicholas, W., Andrew, S., and Robert, B., 2012. Do you see Your Password? Applying Recognition to Textual Passwords. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security* (*SOUPS '12*). Association for Computing Machinery, New York, USA, p8.

Nizamani, S.Z., Hassan, S.R., Shaikh, R.A., Abozinadah, E.A., and Mehmood, R., 2021. A novel hybrid textual-graphical authentication scheme with better security, memorability, and usability. *IEEE Access*, 9, pp.51294-51312.

Por, L., Ku, C., Islam, A., and Ang, T., 2017. Graphical password: Prevent shoulder-surfing attack using digraph substitution rules. *Frontiers of Computer Science*, 11, pp.1098-1108.

Por, L.Y., Ku, C.S., and Ang, T.F., 2019. Preventing shoulder-surfing attacks using digraph substitution rules and pass-image output feedback. *Symmetry*, 11, p.1087.

Rachna, D., and Adrian, P., 2000. Deja Vu--a user study: Using Images for Authentication. In: *Proceeding of the 9th USENIX Security Symposium*.

Rajarajan, S., and Priyadarsini, P.L.K., 2021. SelfiePass: A Shoulder Surfing Resistant Graphical Password Scheme. In: *International Conference on Recent Trends on Electronics, Information, Communication and Technology (RTEICT)*. Bangalore, India, pp.563-567.

Sabzevar, A.P., and Stavrou, A., 2008. Universal Multi-factor Authentication Using Graphical Passwords. In: *Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems*, pp.625-632.

Siddiqui, N., Misbah, U., Mohd, S., and Miftah, S., 2018. A Novel Shoulder-Surfing Resistant Graphical Authentication Scheme. In: *2018 4th International Conference on Computing Communication and Automation* (*ICCCA*). IEEE, pp.1-5.

Sobrado, L., and Birget, J., 2002. Graphical passwords. The Rutgers Scholar. An Electronic Bulletin for Undergraduate Research, 4, pp.1-9.

Sun, H., Chen, S., Yeh, J., and Cheng, C., 2018. A shoulder surfing resistant graphical authentication system. *IEEE Transactions on Dependable and Secure Computing*, 15, pp.180-193.

Susan, W., Jim, W., Jean, C., Alex, B., and Nasir, M., 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1-2), pp.102-127.

Tu, J., Dahai, T., and Yun, W., 2021. An active-routing authentication scheme in MANET. IEEE Access, 9, pp.34276-34286.

Wang, Z., Lingzhi, L., Ruohan, M., Ching-Nung, Y., Zhili, Z., and Hengfu, Y., 2022. Verification Grid and map slipping based graphical password against shoulder-surfing attacks. *Security and Communication Networks*, 2022, p.6778755.

Xiaoyuan, S., Ying, Z., and Scott, G., 2005. Graphical Passwords: A Survey. In: *Proceedings of the 21st Annual Computer Security Applications*, pp.463-472.

Zhao, H., and Li, X., 2007. S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme. In: *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), Niagara Falls, ON, Canada*, pp.467-472.