IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 10, 2021, accepted March 24, 2021, date of publication March 26, 2021, date of current version April 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3069164

A Novel Hybrid Textual-Graphical Authentication Scheme With Better Security, Memorability, and Usability

SHAH ZAMAN NIZAMANI[1], SYED RAHEEL HASSAN[2], RIAZ AHMED SHAIKH[2], EHAB ATIF ABOZINADAH[3], AND RASHID MEHMOOD[4], (Senior Member, IEEE)

[1]Information Technology Department, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah 67480, Pakistan
[2]Computer Science Department, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[3]Information Systems Department, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[4]High Performance Computing Center, King Abdulaziz University, Jeddah 21589, Saudi Arabia

Corresponding author: Shah Zaman Nizamani (shahzaman@quest.edu.pk)

ABSTRACT Despite numerous efforts, developing an authentication scheme that offers strong security while offering memorability and usability remains a grand challenge. In this paper, we propose a textual-graphical hybrid authentication scheme that improves the security, memorability and usability inadequacies of existing authentication schemes. This has been achieved by combining a range of mechanisms together, in a novel manner, to address weaknesses of the existing security schemes. Firstly, two dynamically selectable modes of password entry (Easy Login, and Secure Login) provide a trade-off between usability and security, allowing the user to dynamically switch to any of these methods in real-time based on the security of the surrounding environment (e.g., secure home environment versus insecure public places) or the criticality of the user account (e.g., a bank account). The other mechanisms included a novel use of the drawmetric mechanism for setting the password to improve memorability, multistep authentication, a novel adaptation of one-time password (OTP) concept using a random selection of password elements, random placement of password elements in different steps, assigning random numbers to the password elements to increase security, and use of simple addition to improve security. We have implemented and analysed the proposed scheme for its security against brute-force attacks, dictionary, shoulder surfing, random guessing, phishing or forming, keystroke/mouse logger, and multiple recording attacks. We have also investigated its usability and memorability, reporting various trends of password elements used and the respective authentication times. Moreover, we have compared the proposed scheme with eight other well-known authentication schemes in terms of its resilience and authentication time. The results and analyses demonstrate the effectiveness of the proposed scheme. We believe that a range of novel methods introduced in this proposed scheme opens several doors for innovation in security techniques.

INDEX TERMS Authentication, password security, graphical passwords, textual passwords.

I. INTRODUCTION

The flow of authentication credentials starts from user input into a login screen. The credentials then move through communication media to a system where the stored and user-provided credentials are matched. An authentication scheme must provide password security against various types of attacks. In a textual password scheme, a password can be captured from the login screen by *spyware-based attacks*. A *man-in-the-middle attack* can be launched to steal textual passwords from the communication medium, or passwords may be guessed through *dictionary* or *brute-force attacks* after hacking a password database.

Textual passwords have some natural limitations, such as a limited length in terms of the number of alphanumeric characters and a lack of visual cues for password recall. Due to the limited length of alphanumeric characters, offline guessability attacks will require less amount of time in the future because the power of computing machines is increasing over time [33]. For example, Gosney [17] was able to

The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Chi Chen

crack passwords of windows XP with the help of 25 GPUs in less than 6 minutes. Textual passwords also suffer from human limitations in information memorization. Strong or complex passwords are difficult to memorize, therefore users generally use dictionary words in their passwords. Such passwords are easy to guess through dictionary attacks. Textual passwords are also easy to record because all the alphanumeric characters of a password are directly inserted into the password field.

To improve the security of textual passwords, many graphical password schemes have been proposed. In this type of user authentication, passwords are graphically entered; as a result, many graphical password schemes are susceptible to shoulder surfing attacks. The security and usability of graphical password schemes vary; some schemes are more secure, while others are easier to use [10]. Secure graphical password schemes require a large amount of time and mental effort for authentication. However, easy-to-use authentication schemes have security issues. The reason for this trade-off is that security and usability have conflicting requirements. For example, to reduce authentication time, the password size needs to be small. However, smaller passwords can be easily guessed through brute-force attacks. Therefore, the major challenge in user authentication to achieve a balance between security and usability still holds [29].

Various hybrid schemes have been proposed over the years to address the challenges of textual and graphical passwords [47]. Hybrid schemes use a mix of graphical and textual elements including sketches, lines, grids, drawings, pictures, and text [4], [9], [22]. However, these schemes are vulnerable to attacks such as shoulder surfing [3], spyware [27], and multiple recording attacks [47].

Multi-factor authentication schemes that rely on multiple factors such as user's knowledge, biometrics, user's possessions, etc. have also been proposed to address various security challenges [34], [27], [31]. A well-known example of multi-factor schemes is the schemes that use One-Time Passwords (OTP) for authentication [20], [36]. These schemes may need higher authentication times and are vulnerable to security threats such as man-in-the-middle attacks, malware, phishing, and ATM skimming. Moreover, some of the hybrid and multi-factor schemes require additional hardware for password entry and third-party services [27], [31]. We will review the various authentication schemes in Section II.

In this paper, we propose a novel hybrid textual-graphical authentication scheme that improves the security, memorability and usability inadequacies of existing authentication schemes. This has been achieved by combining a range of mechanisms together, in a novel manner, to address weaknesses of the existing security schemes. The mechanisms include allowing two dynamically selectable methods of password entry to provide a trade-off between usability and security, novel use of the drawmetric mechanism for setting the password to improve memorability, multistep authentication, a novel adaptation of one-time password (OTP) concept using a random selection of password elements, random placement of password elements in different steps, assigning random numbers to the password elements to increase security, and use of simple addition to improve security.

The first mechanism, which is to provide two alternative methods of password entry (the *Easy Login* method and the *Secure Login* method) allow the user to dynamically switch to any of these methods, in real-time, based on the security of the surrounding environment (e.g., a secure home environment versus insecure public places, coffee shops, etc.) or the criticality of the user account (e.g., a bank account). The easy login method is similar to the traditional login methods except that users could select both alphanumeric characters and pictures for their passwords. The pictures are assigned shortcut keys, which are entered using a keyboard. This improves the security of the traditional textual passwords while keeping their usability properties. Our proposed approach for the easy login method improves resilience against brute-force attacks, dictionary attacks, and random guessing attacks.

The secure login method requires a three-step procedure to complete the authentication process. A random selection of the elements of the user's password are presented on the screen in each step of the authentication process. In each of the three steps, the password elements are entered using a simple calculation involving the number of displayed password elements on the screen and the unique numerical values assigned to each of the password elements. Using the secure login method, our proposed approach improves resilience against brute-force attacks, dictionary attacks, shoulder surfing attacks, phishing or forming attacks, keystroke/mouse logger attacks, and multiple recording attacks. Moreover, visual cues are provided on the registration screen to help users to easily memorize strong alphanumeric passwords; i.e., it improves the memorability and usability property of the scheme (this is applicable to both the easy and secure login methods). The scheme does not require additional hardware and therefore provides better usability.

A description of all the mechanisms used in our proposed scheme is given in Section II-F followed by a detailed explanation of the scheme in Sections III and IV.

We have implemented the proposed scheme with a range of login screen layouts and have analysed it for its security, usability, and memorability properties. For security, we have analysed our scheme against seven different types of security attacks including brute-force attacks, dictionary attacks, shoulder surfing attacks, random guessing attacks, phishing or forming attacks, keystroke/mouse logger attacks, and multiple recording attacks. For usability, we have investigated and reported the various trends of password elements used and the respective authentication times. For memorability, we have reported the results of experiments conducted from 154 users. Moreover, we have compared the proposed scheme with eight other well-known password-based authentication schemes in terms of its resilience and authentication time. The results and analyses demonstrate the effectiveness of the proposed scheme.

The proposed scheme includes 118 password elements, 94 of these are alphanumeric characters and the remaining 24 elements are pictures. A user can set a password with elements from the set of all 118 password elements. We describe in this paper one possible implementation of the proposed authentication scheme. Other implementations are also possible, such as with two or more than three steps to enter the password in the secure login method, with different registration and login screens, different ways of placements of pictures and alphanumeric keys in a single page, a different number or kinds of pictures for password entry, the categories of pictures, etc. We have shown in the paper three different ways of placing the pictures on the login screen. It is possible for the developers to provide an implementation of the scheme where the set of pictures, symbols, and alphanumeric elements can be selected or defined by the users.

A clarification: the reason we refer to the scheme as a hybrid textual-graphical scheme is to highlight that it uses both textual and graphical password elements. This hybrid textual-graphical aspect (that does improve the entropy of the password due to its resilience against dictionary, brute force, etc. attacks) alone does not describe the novelty of the scheme rather, as mentioned earlier, the several novel mechanisms used in the scheme and their novel combination represent the novelty of the scheme.

The rest of the paper is organized as follows. In Section II, we review the relevant literature considering different types of textual, graphical, hybrid and multi-factor password schemes. Section III gives a detailed description of the proposed authentication scheme. Section IV gives an illustration, from a user's perspective, of the whole life cycle of our scheme including registration, the easy login method, and the secure login method. Security, usability, and memorability analyses of our authentication scheme are given in Sections V, VI, and VII, respectively. The proposed scheme is compared with eight other well-known authentication schemes in Section VIII. Finally, Section IX gives conclusions and future work.

II. LITERATURE REVIEW

Textual and graphical password techniques are types of knowledge-based authentication schemes, in which users must provide certain information for authentication. Password-based schemes can be divided into five categories based on the types of passwords and methods used. These are recognition-based (searchmetric) schemes, pure recall-based (drawmetric) schemes, cued recall-based (locimetric) schemes, hybrid schemes, and multi-factor authentication schemes. These are reviewed in the following five subsections.

A. SEARCHMETRIC OR RECOGNITION-BASED SCHEMES

Schemes in which a password consists of several pictures are called searchmetric schemes. Dhamija and Perrig [9] proposed a scheme called Deja Vu, in which abstract art pictures are used as password elements. Authentication is performed by selecting the pictures that belong to a password. This scheme is susceptible to shoulder surfing attacks because the password selection process can be easily observed through camera recording. Memorability is also an issue with the Deja Vu scheme, because abstract art pictures are difficult to memorize.

The memorability issues of the Deja Vu scheme are mitigated in the Passfaces scheme [11]. In this scheme pictures of human faces are used for password creation instead of abstract art pictures. The login screen of Passfaces consists of multiple pages, each of which contains nine pictures. For authentication, a user must select the correct password picture on each page. This scheme is susceptible to shoulder surfing and spyware attacks.

Davis *et al.* [8] suggested the Story scheme. In this scheme, images in different categories are used for password creation. The idea of this scheme is that a user creates a story from the password images, which assists in the long-term memorization of the password. The Story scheme has memorability advantages but it is also susceptible to shoulder surfing and spyware attacks.

Wiedenbeck *et al.* [43] proposed a scheme called Convex Hull Click (CHC), in which a password consists of several icons. On the login screen, the user must click inside a logical triangle formed by the password icons. This scheme is resilient to shoulder surfing attacks, but the password icons may be revealed by multiple recording attacks. Lopez *et al.* [28] suggested a shoulder-surfing-resistant scheme. In this scheme, pictures of human faces are used for password creation. On the login screen, three pictures are shown in each row. For authentication, the user must input whether the number of password images in each row is even or odd. This scheme is weak to brute-force attacks because of its small password space.

B. DRAWMETRIC OR PURE RECALL-BASED SCHEMES

In drawmetric schemes, a password consists of several lines or drawings. Jermyn *et al.* [22] proposed a scheme called Draw-A-Secret (DAS). In this scheme, a password consists of several lines on a blank grid-based screen. For authentication, the user must redraw the password lines. This scheme is susceptible to shoulder surfing and spyware attacks.

Dunphy and Yan [12] improved the memorability of the DAS scheme by adding a background to the grid-based login screen. The resulting scheme is called Background DAS (BDAS). The background image provides hints for password recall. This scheme is also susceptible to shoulder surfing and spyware attacks.

Both the DAS and BDAS schemes impose limitations on how the password lines can be drawn, i.e. users can draw only along predefined paths. This restriction is removed in the Passdoodles [38] scheme. In this scheme, users have the freedom to draw any kind of shape such as their own signatures, for password creation. This scheme is also susceptible to shoulder surfing and mouse logger attacks.

C. LOCIMETRIC OR CUED RECALL-BASED SCHEMES

In locimetric schemes, a password consists of several (x, y) coordinates in a picture or a login window. Blonder [4] proposed the first graphical password scheme in which a password consists of several predefined points in a picture. This scheme has a limited password space and is also susceptible to shoulder surfing and mouse logger attacks.

Wiedenbeck *et al.* [42] proposed the PassPoints scheme. This scheme improves the password space of Blonder's scheme by providing a larger number of click points. Although this scheme provides better resistance against brute-force attacks but it is weak against shoulder surfing and mouse logger attacks. This scheme also suffers from a user's tendency to select easy-to-remember points, or ''hotspot'' [37], in a presented picture. An attacker can exploits these hotspots for password guessing.

Chiasson *et al.* [7] further improved the password space of PassPoints scheme by developing a scheme called Cued Click Points (CCP). In this scheme, a password consists of various (x, y) positions in multiple images. This scheme provides a large password space, making brute-force attacks difficult to apply; however, it suffers from hotspots and shoulder surfing vulnerabilities.

D. HYBRID SCHEMES

In the hybrid approach, multiple authentication schemes are combined to improve the security properties of the resulting scheme. Our proposed scheme falls within this category. Zhao and Li [47] proposed a mixed textual and graphical password scheme known as S3PAS. In this scheme, a password consists of traditional alphanumeric characters. On the login screen, all alphanumeric characters are shown in image format. For authentication, the user must search for and click inside the logical triangle formed by the password characters. The S3PAS scheme provides resistance against shoulder surfing attacks, but its passwords may be cracked by multiple recording attacks.

Zheng *et al.* [48] proposed a hybrid scheme based on a password shape and numbers. For password creation, a user draws a shape as in the DAS scheme. On the login screen, various numbers are shown to the user in a grid format. The user must input into the password field the numbers that form the shape of the registered password. This scheme is resilient to keystroke and mouse logger attacks, but its passwords may be broken by shoulder surfing attacks.

Alsaiari *et al.* [3] proposed a spyware-resilient authentication scheme, called GOTPass (Graphical One-Time Password). A passwords in this scheme consists of several pictures and several lines, as in the DAS scheme. On the login screen, pictures are shown along with randomly selected numbers that represent each picture. For authentication, the user must redraw the password lines and input the codes belonging to the password pictures. This scheme is not resilient to shoulder surfing attacks.

Researchers also used audio signals for resisting multiple recording attack. For example, Lee *et al.* [27] proposed an authentication scheme in which a password consists of some digits. For authentication, the system randomly generates an alphabet, which is informed to the user through earphone. The user has to correctly relocate the system generated alphabet in front of the password digit. Due to the use of audio signals, this scheme requires some audio components for execution. Another disadvantage of this scheme is that the passwords consist of only digits, as a result brute force attacks are easy to apply.

Chakraborty and Mondwal [5] proposed an authentication scheme known as colour pass. In this scheme ten colours are shown to the users for password selection. In the login screen, ten tables are shown and each cell of the tables has different colour and a unique numeric representation. A password is entered by typing some numbers which represent the colours of a password, based upon the table number randomly generated by the system. The table number is transferred to the user though headphone. This scheme is resilient to shoulder surfing attack but it requires some external hardware for execution, and the scheme also contains small password space.

E. MULTI-FACTOR AUTHENTICATION

In a multi-factor authentication scheme, a user is granted access to a resource based on two or more sources or factors including, among others, user's knowledge, biometrics, user's possessions (e.g., a specific device), user's location, and the time of authentication [34]. Several recent authentication schemes use multi-factor authentication methods [21], [23], [30] for improving the security of the authentication process.

Some of the multi-factor authentication schemes use approaches based on one-time passwords (OTP) where an additional device and/or third-party services are required [20], [24], [36]. For example, Sorochi *et al.* [36] proposed a multi-factor authentication scheme for automatic door unlocking. In this scheme, a user is registered with a traditional textual password and a mobile number. At the login time, the user provides a password in a dedicated login screen. The system verifies the password and sends a code through an SMS service if the password is correct. The door is unlocked if the user correctly enters the code received through the SMS. Another example of a multi-factor scheme based on the OTP approach is the scheme proposed by Kansuwan and Chomsiri [24], where a user is registered with a username, a password, and a CAPTCHA. At the login time, the user provides all the registered information (the username, password, and CAPTCHA). The authentication system sends a one-time password to the user through SMS or email after verifying the information. The user is authenticated after correctly entering the received OTP in a login screen.

Some multi-factor authentication schemes use dedicated hardware for authentication. The ESEAP scheme [25] is an example. In ESEAP, a user's identity is verified using a traditional textual password and hardware called a smart card. The authentication process completes in two phases. In the first phase, the user inserts the smart card into a dedicated

machine, which establishes a connection to the authentication server. In the second phase, the user provides the registered password for authentication.

The use of additional hardware, added communication over networks, and the use of third-party services add to the authentication time and increases vulnerability against various attacks including man-in-the-browser, man-in-the-middle, malware, and phishing attacks. We will provide a comparative discussion between multi-factor schemes and our proposed scheme in Section VIII-C.

F. RESEARCH GAP

The literature review given above has revealed the weaknesses of the current password schemes. Recognition-based (searchmetric) schemes are weak against shoulder surfing, spyware, and brute force attacks, and have usability issues. Pure recall-based (drawmetric) schemes suffer from shoulder surfing, spyware, mouse logger attacks, and poor memorability. Cued recall-based (locimetric) schemes struggle against password guessing, mouse logging, and shoulder surfing attacks. Hybrid schemes are vulnerable to shoulder surfing, spyware, and multiple recording attacks, and may also require higher authentication times.

Multi-factor schemes are vulnerable to some security threats such as man-in-the-middle attacks, malware, phishing, and ATM skimming. They usually rely on third-party services such as email or SMS for authentication and hence typically need higher authentication times. Moreover, multi-factor schemes, and some of the hybrid schemes, require additional hardware for password entry and hence could be considered to have poor usability.

The scheme proposed in this paper mitigates the effects of all the above-mentioned attacks and provides better security, usability, and memorability compared to the current schemes. This has been achieved by combining a range of mechanisms together, in a novel manner, to address weaknesses of the existing security schemes. The mechanisms include allowing two dynamically selectable modes of password entry to provide a trade-off between usability and security, novel use of the drawmetric mechanism for setting the password to improve memorability, multistep authentication, a novel adaptation of one-time password (OTP) concept using a random selection of password elements, random placement of password elements in different steps, assigning random numbers to the password elements to increase security, and use of simple addition to improve security. We briefly elaborate this as follows; a detailed elaboration of the scheme is given in Sections III and IV.

The proposed scheme provides a novel concept of facilitating two dynamically selectable modes of password entry to provide a trade-off between security, memorability, and usability. The user could dynamically switch to any of these methods based on the security of the surrounding environment (e.g., a secure home environment versus insecure public places, coffee shops, etc.) or the criticality of the user account (e.g., a bank account). We have not seen any current scheme in the literature or practice with two such alternative methods of authentication.

The way in which the drawmetric approach is used in our scheme is novel because it helps in memorizing a random or complex alphanumeric password and improves authentication security (see Section III-C, Section V-A1, and Figures 3 and 6). Drawmetric approaches are very useful in creating passwords that are almost impossible to be broken by dictionary and brute force attacks. The drawmetric approach in our case is only used for creating passwords and for the Easy Login method and therefore does not affect the security of the Secure Login method. Note that the drawmetric approach is optional and the user can set a password without using it.

The multistep mechanism has been introduced in the Secure Login method of the scheme to provide robustness against guessability and session recording attacks. In the current implementation of the proposed scheme, three password entry steps are used but the number of steps can be increased based on the criticality of the user account. A higher number of steps are likely to affect the usability of the proposed scheme including the login time (see Section IV-C and Figure 8).

The mechanism in which we have implemented OTP is novel. As mentioned earlier, multi-factor authentication schemes utilize the benefits of OTP approaches but, in doing so, they inherit dependency on third-party resources (SMS, email, dedicated hardware, etc.), and, in turn, this weakens the usability and security of the schemes (see Section VIII-C). The proposed scheme avoids usability and security issues of multi-factor authentication techniques. A user does not need to receive a password from any third-party source, instead, the password is calculated from the secure login screen, and, therefore, the passwords cannot be recorded. The OTP adds to the proposed scheme's robustness against different spywares, keyloggers, and shoulder surfing attacks which are becoming easier and prevalent due to the ubiquity of surveillance cameras. Also, the proposed scheme is efficient to use because it does not require any additional hardware for authentication.

We have used the multistep mechanism to randomize the disclosure or visibility of the password elements in each step to add another complex layer of security. While entering the password in each step, a few of their password elements are visible to the user. This mechanism protects against the disclosure of all the password elements at one time and gives protection against shoulder surfing and session recording attacks. For further details, see Section III-D, and Figures 4 and 5.

The assigning of a random number to each visible element on the screen is a novel trick that adds more work for the attacker in cracking the password elements. These random numbers increase the password cracking time if the attacker is using automated tools to calculate the entered number. This mechanism in our scheme also provides robustness against shoulder surfing and recording attacks (see Section III-D, and Figures 4 and 5).

The role of simple addition in the proposed scheme is to make the number calculations complex and time consuming for the attackers. For the user it is very simple as the user will have to add the number visible on top of the last visible password element with the number visible on top of each password element. The addition is very simple and does not require any calculating device.

See Sections III and IV for details on all of the mechanism discussed above.

III. THE PROPOSED AUTHENTICATION SCHEME

The proposed scheme includes two common phases for user authentication, namely, the registration and login phases. On the registration screen, passwords are entered with the keyboard or mouse. To improve password memorization, users are given the option to create passwords by drawing patterns on the registration screen.

The proposed scheme provides two different methods of entering the password, Easy Login and Secure Login, to provide a trade-off between security, memorability, and usability. The user could dynamically switch to any of these methods based on the security of the surrounding environment or the criticality of the user account. The easy login method is similar to the traditional login methods except that users could select both alphanumeric characters and pictures for their passwords. The pictures are assigned shortcut keys, which are entered using a keyboard. The secure login method requires a three-step procedure to complete the authentication process. A random selection of the elements of the user's password are presented on the screen in each step of the authentication process. In each of the three steps, the password elements are entered using a simple calculation involving the number of displayed password elements on the screen and the unique numerical values assigned to each of the password elements.

Note that we describe in this paper one possible implementation of the proposed authentication scheme. Other implementations are also possible, such as with two or more than three steps to enter the password in the secure login method, with different registration and login screens, different ways of placements of pictures and alphanumeric keys in a single page, a different number or kinds of pictures for password entry, the categories of pictures, etc.

The registration phase and the login phase are described in Sections III-A and III-B, respectively. The easy login method (Section III-C) and the secure login method (Section III-D) are described next, followed by the implementation details in Section III-E.

A. REGISTRATION PHASE

The proposed scheme includes 118 password elements, 94 of which are alphanumeric characters, while the remaining 24 elements are pictures (the number or types of pictures can be changed). A user can set a password from the list of all 118 password elements. The alphanumeric characters are shown on the "Alphanumeric" tab, while the pictures are shown on the "Figures" tab of the registration screen,

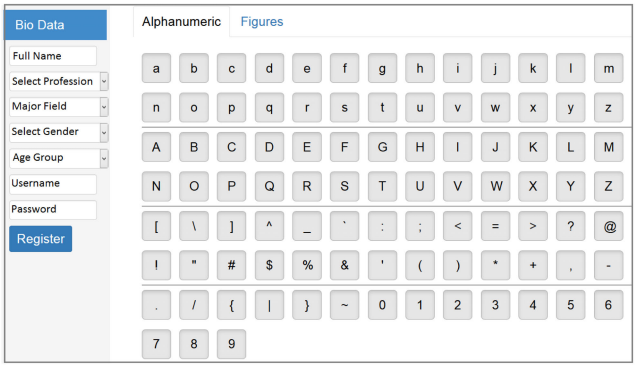


FIGURE 1. Registration screen with alphanumeric characters.

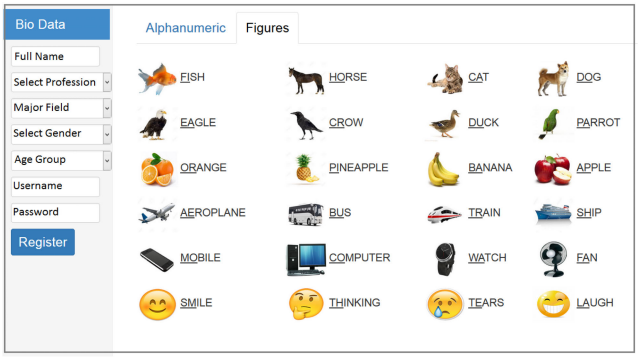


FIGURE 2. Registration screen with pictures.

as shown in Figures 1 and 2. Fields for profile information are given in the left side of the registration screen. The registration phase starts when a new user enters profile and authentication information on the registration screen.

Note in the figures that the password pictures are divided into six categories (animals, birds, fruits, vehicles, electronics, and emojis), each of which contains four images. As mentioned earlier, the specifics of the implementation of the scheme, such as the number of categories of the pictures can be changed. In the database of the proposed scheme, these pictures are represented by Unicode symbols. For example, the picture of a "fish" is represented by 'α'. These symbols may be modified with different implementations of the proposed scheme. Passwords may consist of alphanumeric characters, pictures or combination of both.

Password Entry: On the registration screen, a password is input with the keyboard or mouse. A user can type a password using the keyboard, as in an traditional textual password scheme. A password picture is input through the keyboard by means of a shortcut key, which consists of ctrl + alt + the first two letters of the picture title. For example, the password image "fish" is input by typing "ctrl+alt+fi". By contrast, mouse-based password entry requires clicking or dragging the mouse over the password elements as shown in Figure 3. A line connecting the password elements is generated when a password is created by mouse dragging. This line assists in memorizing the alphanumeric characters and pictures of a password.

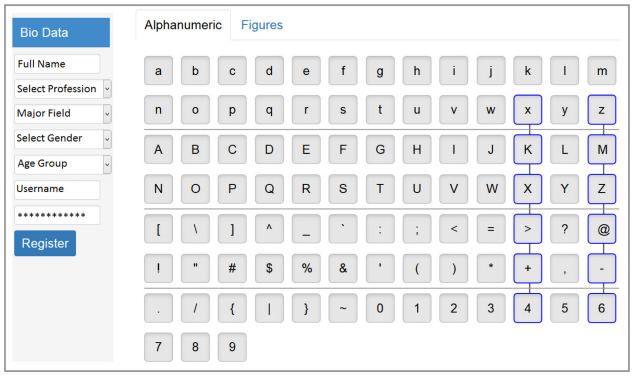


FIGURE 3. Password selection on the registration screen.

Dragging the mouse from top to bottom generates a different password than dragging from bottom to top, although visually both passwords will have the same shape. To add an element multiple times, a user must click or type that element more than once. For example, the password "aaaa" is entered by clicking or typing the character "a" four times.

Passwords created through mouse dragging are generally secure and easy to memorize. For example, the password "x K X > + 4 z M Z @ - 6" can be easily remembered by memorizing the two lines from "x" to "4" and from "z" to "6" as shown in Figure 3. This password is more secure because it has a high password entropy.

B. LOGIN PHASE

The proposed scheme offers two methods of authentication. The first is called easy login, while the other is called secure login. In the easy login method, minor security improvements are made for authentication but it is easy to use. While major security improvements are made for authentication in the secure login method, as a result this method requires a little more time and mental effort for password input. Developers and users have the choice to select any of the login methods. Developers can implement any one or both the login methods (easy or secure) depending upon the type of application. Only secure login method is recommended for the applications which store sensitive data. When both login methods are implemented, users have the choice to select either method depending on the authentication environment, which may be secure or insecure. A *secure environment* is one in which a user is using a private device and a private network with no chance of shoulder surfing attacks, for example, a home network. An environment in which a user is using a public device or network with a high chances of shoulder surfing attack is called an *insecure environment*; examples include airports or cafeterias. The easy login method is recommended for secure environments because the chances of security attacks are low. Users may find the easy login method suitable for less sensitive applications such as blogs and newsletters. The secure login method could be used for insecure authentication environments or for applications such as e-banking and e-commerce.

C. EASY LOGIN METHOD

The login screen of the proposed scheme contains two password fields, as shown in Figure 4: one for secure login and the other for easy login. The password entry process in the easy login method is the same as in a traditional textual password scheme. The user must input the username and registered password in the text field labeled as "Complete Password" and press the "Submit" button. Password pictures are input via shortcut keys, as on the registration screen. The alphanumeric characters and pictures that are visible in the right-hand section of the login screen are used for the secure login method.

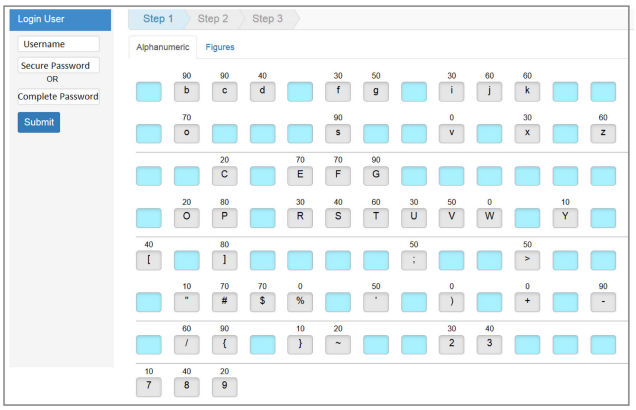


FIGURE 4. Login screen with alphanumeric characters.

D. SECURE LOGIN METHOD

The secure login method is resilient to various observability and recordability attacks. This method consists of three steps; in each step, the user must enter a number, instead of registered password in the text field labeled "Secure Password". The process of authentication through the secure login method is divided into three parts: login screen generation, password input, and password matching.

1) SECURE LOGIN SCREEN GENERATION

For the secure login method, 50% of the elements (alphanumeric characters and pictures) are randomly selected for display, and numeric values are assigned to all selected elements from a pool of 10 numbers (0, 10, 20, . . . , 90). These numeric values are presented above the visible alphanumeric characters and to the right of the pictures as shown in Figures 4 and 5. Left side of the login screen contains one field for username and two fields for password insertion. Password of the secure login method is entered in the field known as "Secure Password" as shown in Figure 4.

The login screen consists of three steps or tabs for secure login method. In all the three steps, randomly 50% elements are presented along with the numeric values. The list of the selected password elements and their assigned values is saved in a session variable for password matching.

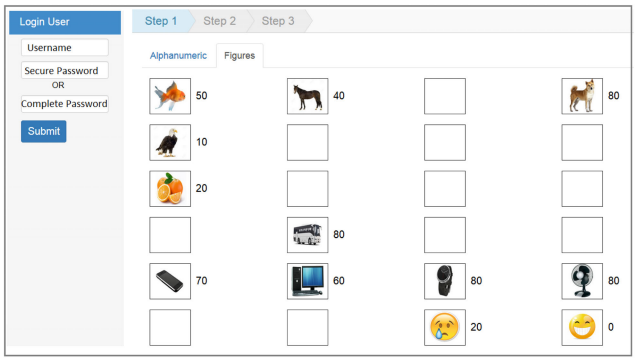


FIGURE 5. Login screen with pictures.

To allow users to quickly locate the password elements on the login screen, the alphanumeric characters are presented in their natural order. The password pictures are presented by category. For example, all animal pictures are presented in the same row.

2) SECURE LOGIN PASSWORD ENTRY PROCEDURE

In the secure login method, a password is represented by some decimal numbers that are entered in the text field labeled as "Secure Password". Login session completes when a user enters username and password number for all the three steps of the secure login screen.

The three-step procedure is elaborated in the following using the password "x K X > + 4 z M Z @ - 6" (see Figure 4).

Step 1: (a) The user enters the username. **(b)** The user counts the number of visible elements (alphanumeric characters and pictures) that belong to the password on the login screen appearing in Step 1 of the secure login. In this case, the count is "5" because the visible password elements on the login screen are "x > + z -" (see Figure 4). **(c)** The user locates the value assigned to the last visible password element. In this case, the last visible password element is '-', and its assigned value is "90". **(d)** The user adds the number of visible password elements counted in "b" above to the assigned value of the last visible password element identified in "c". In this case, the count is "5" and the assigned value of the last visible password element is "90". The sum of the two numbers is "95". **(e)** The user enters the password number calculated (in this example, "95") into the password field and clicks the "Submit" button, which moves the user to Step 2.

Step 2: The same actions (given in Step 1 above) are repeated in Step 2 up until the user clicks the "Submit" button, which moves the user to Step 3.

Step 3: The actions in Step 1 are repeated in Step 2 up until the user clicks the "Submit" button, which authenticates and logins the user to the system.

Note that Figure 4 only shows password elements for Step 1. We will elaborate the whole password entry procedure for a password comprising textual and picture elements in Section IV.

E. IMPLEMENTATION OF PASSWORD MATCHING PROCEDURE

We now explain the implementation of the secure login procedure as to how the input password numbers and username are matched with the credentials stored in the database. Password matching is performed as follows.

Step 1: (a) The server receives the username and the password number entered for the first step of the secure login method. Based on the username, the system fetches the corresponding password from the database. **(b)** The system counts the number of visible elements belonging to the user's password on the login screen. **(c)** The system identifies the value assigned to the last visible password element. **(d)** The system generates a number by adding the number of visible password elements on the screen and the numeric value of the last visible password element on the screen. **(e)** The system compares its generated number in "d" with the number entered by the user. If the number is correct, it generates the screen for Step 2.

Step 2: The procedure given in Step 1 is repeated for Step 2. The system generates the screen for Step 3 on a successful password entry.

Step 3: The procedure given in Step 1 is repeated for Step 3. The system authenticates the user on a correct password entry.

IV. A COMPLETE REGISTRATION AND LOGIN EXAMPLE

To sum up and elaborate on the earlier discussions, we give here an illustration of the whole cycle of our scheme including registration, the easy login method, and the secure login method. The previous section has described various aspects of the proposed scheme including its design and implementation. In this section, we illustrate the scheme from the users' perspective. We use a password as a running example in this section. The password comprises both textual and graphical elements. The password contains five alphanumeric characters (qDR#9) and four pictures (cat, orange, apple, and mobile); see the bottom left part of Figure 6.

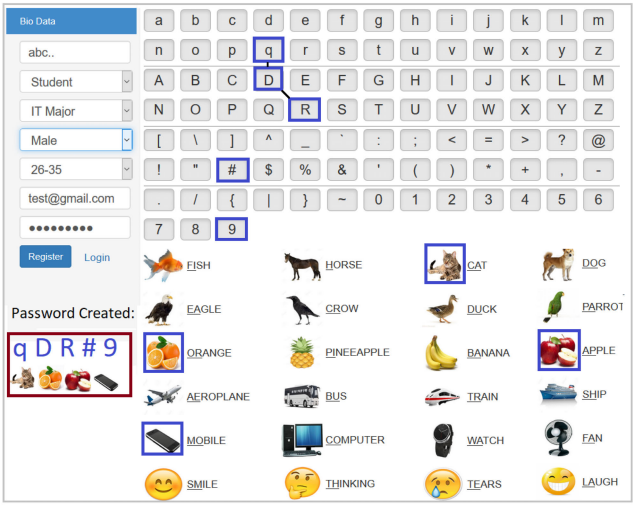


FIGURE 6. Password Registration.

A. PASSWORD REGISTRATION

During registration, a password can be selected through a keyboard or mouse. When using a keyboard, a password can be set by typing alphanumeric keys and specific shortcut keys assigned to the pictures. We have illustrated the registration process in Figure 6 for the password that we are using as the running example — five alphanumeric characters (qDR#9) and four pictures (cat, orange, apple, and mobile). The password can be entered by typing the alphanumeric characters (qDR#9) and using the specific shortcut keys of the pictures. The shortcut keys for the four pictures are 'ctrl+alt+ca', 'ctrl+alt+or', 'ctrl+alt+ap' and 'ctrl+alt+mo', respectively. All the selected password keys get highlighted in blue square boxes as shown in Figure 6. The highlights only appear in the registration screen and do not appear in the login process. Moreover, the password shown on the left side of the screen is for illustration purposes only and will not appear in the actual case. Note in Figure 6 that the textual elements and the pictures are shown on the same screen in contrast to Figure 2 where the textual elements and pictures are provided in different tabs. This is because we have developed multiple layouts of the screens (see also Figure 7) to show the various possibilities from a usability perspective.

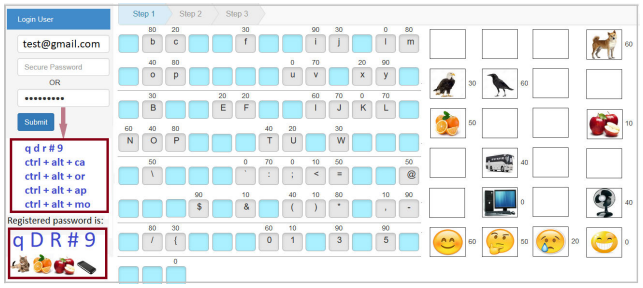


FIGURE 7. The Easy Login Method.

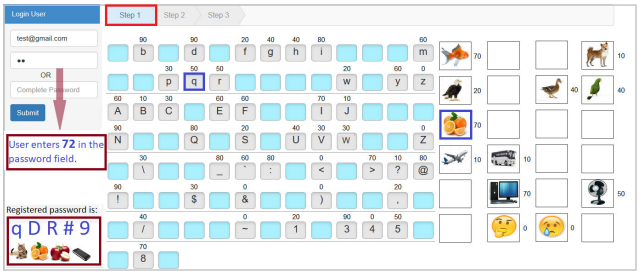
When using a mouse for entering a password, the user needs to click or drag the mouse on the alphanumeric characters or pictures present in the registration screen. The running example password can be selected by dragging the mouse from "q" to "R" and clicking on the password elements "#9" and pictures of the cat, orange, apple, and mobile. Note in Figure 6 that the lines between the three password elements "q" to "R" are due to dragging the mouse.

B. THE EASY LOGIN METHOD

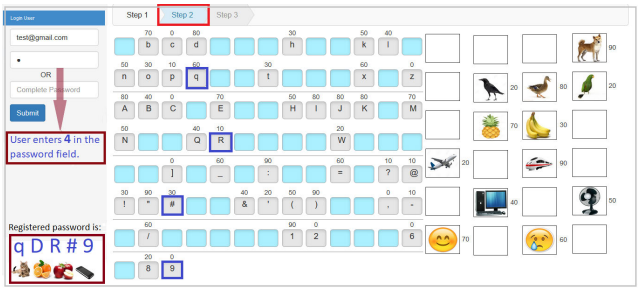
The screen for the easy login method is shown in Figure 7. It contains one username field and two fields to enter the password (see top left of the screen). While using the easy login method, the user will enter the password in the second field (at the bottom). The top field below the username field is for the secure login method. In the easy login method, a password can only be entered through a keyboard. The running example password will be entered by pressing five alphanumeric keys (qDR#9) and the four shortcut keys specific to the pictures; 'ctrl+alt+ca', 'ctrl+alt+or', 'ctrl+alt+ap' and 'ctrl+alt+mo', respectively. This is illustrated in Figure 7 on its left side. Note that, in contrast to the registration screen, no password elements are highlighted in the login process.

C. SECURE LOGIN METHOD

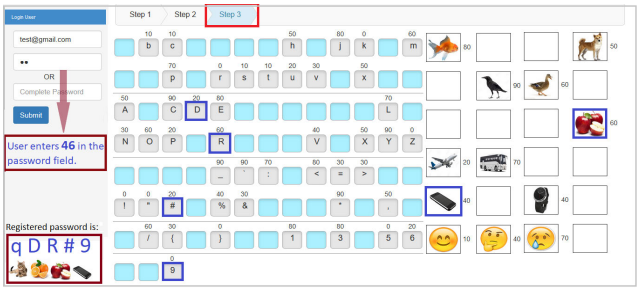
The screen for the secure login method is the same as for the easy login method. However, as has been explained in the previous section, the secure login requires three steps for authenticating the user. Figure 8 shows three screens, one for each step.



(a) Step 1 of the Secure Login Method



(b) Step 2 of the Secure Login Method



(c) Step 3 of the Secure Login Method

FIGURE 8. The Secure Login Method.

Step 1: In the first step, the user enters the username and a number based on the password elements visible on the screen; see Figure 8(a). Considering the running password example, and the password elements displayed in Figure 8(a), the user will enter the value "72" in the secure password field. The screen in Step 1 has only two visible password elements, 'q' and the picture of 'orange', giving us the value '2'. The value associated with the picture 'orange' is 70 (see Figure 8(a)). Adding '2' and '70' gives us 72. Note in all the three subfigures in Figure 8 that the selected password elements are

TABLE 1. Questions regarding traditional passwords.

S. No.	Question	Response
1	What is the length of your most frequently used password?	Any Integer
2	Does your password contain lower-case letters?	Yes / No
3	Does your password contain upper-case letters?	Yes / No
4	Does your password contain numbers?	Yes / No
5	Does your password contain special characters?	Yes / No

highlighted with blue square boxes. These are for illustration purposes only and will not be highlighted during the actual login process.

Step 2: The second step is the same as the first step. The user will enter a value based on the visible password elements. Four password elements (''qR#9'') are visible in Figure 8(b) and the value associated with the last password element is '0'. The user enters '4' (i.e., ''4 + 0'') in the password filed.

Step 3: Six password elements (''DR#9'' and pictures 'apple' and 'mobile') are visible in the third step; see Figure 8(c). The value associated with the last password element is '40'. The user enters '46' (i.e., ''6 + 40'') in the password filed. This completes the secure login process and would authenticate the user.

In the secure login process, a user can either use a keyboard to move through the three steps using the tab key, or both a keyboard and a mouse.

V. SECURITY ANALYSIS

Security is the prime focus of authentication schemes, and passwords can be breached through various types of security attacks. Below, the security of the proposed scheme is analyzed with respect to seven different security attacks including Brute-Force Attacks, Dictionary Attacks, Shoulder Surfing Attacks, Random Guessing Attacks, Phishing or Forming Attacks, Keystroke/Mouse Logger Attacks, and Multiple Recording Attacks.

A. BRUTE-FORCE ATTACK

A brute-force attack is an offline attack in which the attacker tries all password combinations to guess one or more passwords. The time required to break a password through a brute-force attack depends on the password space and the strength of the password. For example, a password consisting of six lower-case alphabetic characters requires 26^6 guesses when the encryption technique and salt string are known.

To analyze the effort required to crack passwords in the proposed scheme compared with traditional textual password scheme, a user study was conducted. The user study consisted of two phases. In the first, a pretest questionnaire was given to the participants. In the second phase, the participants registered and logged into a web-based application using an authentication scheme similar to the proposed scheme. The textual password scheme used in these and other experiments reported in this paper was implemented as a web-based application with a standard US keyboard. For both phases, 80 users from different backgrounds were selected from Quaid-e-Awam University of Engineering Science and Technology.

In the pretest questionnaire, the participants were asked various questions about their most frequently used passwords. They were asked to specify the password length and the types of alphanumeric characters used in their passwords. Table 1 shows the list of questions asked during this phase. The purpose of this activity was to assess the strength of traditional textual passwords.

For the application testing phase, the participants were asked to open a link to a web-based application that was developed to test the behavior of users interacting with the proposed scheme. In this testing application, two pages were created, one for registration and the other for login (these pages have been discussed and shown in Figures 1 and 4, respectively). A demonstration of the registration and login activities was given to the users, and they were then asked to perform the registration and login activities. In the application, only one restriction was imposed on the creation of passwords, namely, a minimum password length of six elements.

1) PASSWORD ENTROPY COMPARED TO TEXTUAL PASSWORDS

Table 2 compares the entropy and average password length of the proposed scheme with textual password scheme. The entropy is calculated using Equation (1), taken from [16].

$$Entropy = log_2 S^L \tag{1}$$

where S is the size of the pool of unique possible symbols (character set), L is the password length, and S^L represents the number of possible combinations. The average password length reported in Table 2 is calculated using the information collected from the user study mentioned in Section V-A.

TABLE 2. Password strength comparison.

Scheme	Entropy	Average Password Length
Textual password	53.88 bits	9.56
Proposed scheme	59.42 bits	9.11

Table 2 shows that the password entropy of the proposed scheme is higher than that of textual password scheme, while the average password length is almost the same as that of textual passwords. This high entropy indicates that the passwords in the proposed scheme were created by mixing different alphanumeric characters, pictures and pattern-based approach in the registration screen. High entropy passwords

are better for security because such passwords rarely present in the password dictionaries and brute force attack will require more effort for password cracking.

Some clarification on the impact of draglines on password entropy follows. Password memorability is degraded for high-entropy passwords. In the proposed scheme, this issue of providing both high memorability and entropy is addressed using a pattern or drawing-based approach for setting up the password by selecting alphanumeric characters and images. Based on the specific implementation of the scheme, the password elements (images and characters) on the registration and login screens can be arranged in different combinations and in different numbers of horizontal and vertical lines. The draglines drawn by the users do not have to be straight. These could be horizontal, vertical, zigzag, arc-shaped, alphabet-shaped, etc. Moreover, the draglines drawn by the users comprising characters and images could also be based on certain visual patterns such as a snake made with straight or curved lines, a rectangle, a mathematical operation (e.g., the division operation), a two- or three-digit number (e.g., the number ''11'' shown in Figure 3), and so on. There is no limit here, virtually, and anything is possible based on the users' imagination. A simple drawing of a snake or bird can have completely different visual patterns based on how two users perceive the visualization of a snake or a bird (e.g., a user may perceive a bird as a straight horizontal line with two small vertical lines coming upwards and downwards from the middle of the horizontal line, and this is easy to remember but difficult for another person to guess and hence would have high entropy).

In the experiments reported in this section, the users mostly drew vertical lines for setting their passwords, and as a result, the passwords were mixed with small and capital characters along with symbols and numbers. This is why we claimed that a relatively high entropy was achieved by our proposed scheme. Using other shapes such as an alphabet-shaped (e.g., L, T, X, etc.) drag for selecting password elements may result in even higher password entropy. The majority of users had set passwords with three lines. A single drag action will result in one or more than one character or image.

2) RESILIENCE TO PASSWORD CRACKING COMPARED TO TEXTUAL PASSWORDS

We now compare the numbers of brute force attacks (or attempts) required to crack the passwords in the proposed scheme with textual password scheme. In these experiments, the salt string and hashing method were known. We have mentioned earlier in this section that the results were collected from the survey conducted by 80 university students. The results are depicted in Figure 9 and show that a higher percentage of passwords can be cracked in textual password scheme compared to the proposed scheme when the same number of guesses are applied in a brute-force attack. The figure contains seven pairs of results related to seven pools containing various numbers of random password elements ranging between $1E + 14$ (10^{14}) and $1E + 38$ (10^{38}).

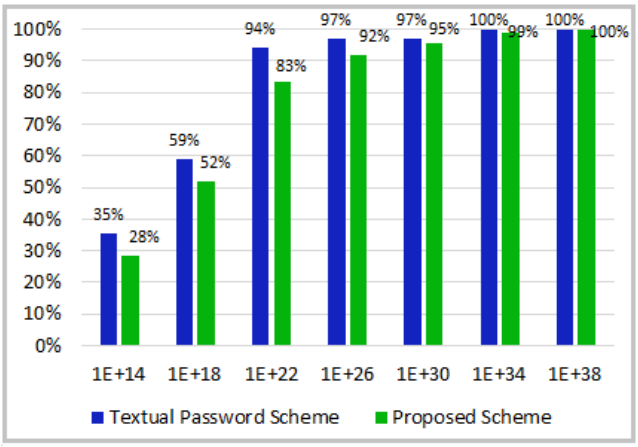


FIGURE 9. Resilience to Password Cracking (Proposed Scheme vs. Textual Passwords).

The results for the textual password scheme and the proposed scheme are plotted with blue and green bars, respectively.

The leftmost pair of bars in Figure 9 shows the results for the case where the students had selected a password containing six elements drawn from the pool of $1E + 14$ random password elements. Note in the figure that 35% of the textual passwords were cracked compared to 28% of passwords in our proposed scheme. The improved performance of our scheme is due to the inclusion of figures and randomization of the password elements enabled by the proposed scheme. The pair of bars labelled $1E + 18$ represents the results for the case where the students had selected a password containing eight elements drawn from the pool of $1E + 18$ random password elements. Note that 59% of the textual passwords were cracked compared to 52% of passwords in our proposed scheme.

The next five pair of results in Figure 9 relate to the cases where the students had selected passwords containing 10, 12, 14, 16, and 18 elements drawn from the pool of $1E + 22$, $1E + 26$, $1E + 30$, $1E + 34$, $1E + 38$ random password elements, respectively. Note in the figure that our proposed scheme consistently provides better performance than the textual password scheme up until the last pair of results where 100% of the passwords from both textual and the proposed scheme are cracked. As mentioned earlier, the improved performance of our scheme is due to the inclusion of figures and randomization of the password elements enabled by the proposed scheme. In the current implementation of the proposed scheme, we have a limited number and types of figures. An increase in the number of figures will make password cracking more difficult and will provide even better performance for the proposed scheme.

B. DICTIONARY ATTACK

In this attack, a password is cracked by comparing the password of a user against a pregenerated list or dictionary of passwords. The probability of a successful dictionary attack depends on the size of the password dictionary. In traditional

textual password scheme, users generally use dictionary words or personal names in their passwords and also reuse passwords among different accounts. This behavior makes passwords easier to memorize, but attackers can also utilizes this information to create password dictionaries.

To analyze the effect of dictionary attacks on the passwords created in the proposed scheme, the John the Ripper [1] password cracking application was used. The data set for the dictionary attack was taken from four sources, which are listed in Table 3.

TABLE 3. Password Dictionaries.

S. No.	Source	Wordlist Size
1	RockYou application	32 million
2	Openwall Project	40 million
3	MySpace application	45 thousand
4	Google web corpus	14 million

Passwords with images were excluded from this experiment because image-based passwords do not exist in the source password dictionaries. After the dictionary attack, only 9.45% of the alphanumeric passwords were cracked based on the wordlists, which contained approximately 86 million unique passwords.

C. SHOULDER SURFING ATTACK

In a shoulder surfing attack, a login activity is observed or recorded. When the easy login method is used, a password can be captured through camera recording. However, passwords entered using the secure login method cannot be revealed in this way because the exact password elements are not entered in the password field.

D. RANDOM GUESSING ATTACK

The easy login method is not susceptible to random guessing attacks because the chance of correctly guessing all password elements is very low. However, in the secure login method, there is a minor chance that all password numbers may be correctly guessed. We calculate the probability of a successful random guessing attack in the secure login method by Equation (2).

$$P(S) = (1/(90 + L))^N \tag{2}$$

Here *'L'* is the length of the password, and *'N'* is the number of steps in the secure login method. The two-digit number "90" is the maximum value assigned to any element (alphanumeric character or picture). For example, if the password consists of 10 elements and three steps are required for authentication, then the probability of a successful random guessing attack is given by Equation (3).

$$P(S) = (1/100)^3 \tag{3}$$

E. PHISHING OR FORMING ATTACK

In a phishing attack, a user is redirected to a fake website and asked to enter a password. The attacker then records this password. The easy login method is susceptible to this attack, but the secure login method is not because the password cannot be revealed by the three decimal numbers entered by the user.

F. KEYSTROKE/MOUSE LOGGER ATTACK

Keystroke loggers send keypress information to an attacker, while mouse loggers send the (x, y) coordinates of mouse click positions. Passwords entered using the easy login method can be revealed by keystroke logger attacks because the user types exact password elements. However, secure login method is resilient to keystroke/mouse logger attacks because random numbers are entered into the password field. Thus, the real password cannot be deduced from keystroke logger information.

G. MULTIPLE RECORDING ATTACK

In this attack, a password is cracked by obtaining information from multiple login sessions through spyware applications such as screen scrappers, keystroke loggers or mouse loggers. For the easy login method, a recording of a single login session may be sufficient to crack a password, but for the secure login method, many recordings are required. The secure login method improves password security against multiple recording attacks by hiding 50% of all the elements (alphanumeric characters and pictures) on the login screen and using two-digit numbers to represent the elements.

An attacker may break a password entered using the secure login method by sequentially cracking each password element. On the login screen each two-digit value is assigned to six elements; therefore, after recording one login session, the attacker has a probability of 1/6 of guessing a password element. A probability of 100% is achieved when intersection of two or more recorded sets yields a single element. This situation is mathematically represented in Equation (4).

$$A \cap B = C \quad and \ |C| = 1 \tag{4}$$

Here, *'A'* and *'B'* denote the two sets of elements captured by recording two login sessions, and *'C'* denotes the intersection of these two sets. A password element is cracked when the cardinality of *'C'* becomes *'1'*. The set of elements (for example A) can be captured by following the steps:

1) An attacker captures the password number and screen-shots of the login screen for a particular session. For example, captured password number is "95" and screen-shots are same as shown in Figures 4 and 5.
2) The attacker identifies all the elements in the screen-shots of the login session, which has assigned the number "90". Note that additional five numbers $(90 + 5 = 95)$ show the count of password elements visible in the login screen. Similarly, if the attacker had captured the password number "37" then the attacker would have to identify all the elements belong to the number "30".
3) Based upon the number "90" and screen-shot shown in Figures 4 and 5, the attacker will identify "b, c, s, G, -, {" elements. These elements will be part of set "A" for multiple recording attack.

4) All the above steps will be repeated after recording second login session for capturing elements of set B.

After performing intersection operation if the cardinality of two sets (A and B) is not '1', then the attacker must recursively perform many intersection operations until the cardinality becomes '1'. Such recursive intersections are represented in Equation (5).

$$C_{i-1} \cap B_i = C_i \quad where\ i \in \{1, 2, 3, \ldots n\} \tag{5}$$

Here, B_i is the set of elements from the most recent recording and C_{i-1} is the intersection of all previous sets of elements. The complete password is cracked when all password elements are sequentially captured through this intersection process, which requires recordings of several hundreds of login sessions. For example, if two elements (c, -) remains after the intersection of two sets A and B, then elements of the third login session will be intersected with the result of the previous set (for example c, -). The process of intersection continues until a single element remains after the intersection. Longer passwords will require more recordings to crack in a multiple recording attack.

Through the intersection process, initially last password element will be cracked after that second last element will be cracked. However, in order to crack second last element, the screen-shots of the login session must not contain last element of a user's password. Similarly, for cracking third last element, the screen-shots must not contain last two elements of a user's password and so on. In the best case scenario, for successfully applying multiple recording attack on the password of size n, at least 2^n recordings of login sessions are required.

VI. USABILITY ANALYSIS

The usability and memorability of the proposed scheme were analyzed using the web-based application mentioned in section V-A. This application was developed using the "PHP" programming language and a "MySQL" database. Various processes were implemented in the application to store registration timings, login timings, and password entropies. Once the test results were collected from the application database, further analyses were conducted.

A. TESTING PROCEDURE

The testing procedure was divided into three sessions. In the first session, the participants performed both the registration and login activities. The second session was held one day after the registration, and the users performed only the login activity. In the last session, which was held one week after registration, the same users again performed the login activity. Only three attempts were allowed for authentication; if a user was not able to login after three attempts, then that user was considered to have failed in the login activity. The users were given the freedom to create a password through either the keyboard or mouse. The minimum password length was set to 6 elements. For authentication, the users were asked to sign in with both the easy login and secure login methods.

Before starting the first session, an introduction to the proposed scheme was given to the participants. After this introduction, all testing activities (registration and login) were explained and demonstrated to the participants. When all participants fully understood how to perform the testing activities, every participant was asked to perform the tests.

B. EXPERIMENTAL RESULTS

After all sessions were completed, the collected data were imported from the database of the testing application. The data were analyzed to identify the password trends and activity timings of the proposed scheme.

1) PASSWORD TRENDS

Different types of passwords selected by the 160 users are given in Table 4. The results show that the majority of the passwords were created through mouse dragging or pattern drawing. The pattern or line-based passwords were mostly created by dragging mouse from top to bottom over the alphanumeric characters. For better memorability, users created different symbols of alphanumeric characters for the pattern or line-based passwords. The results also show that very few users selected images for password creation; this we believe is due to their established habit of creating textual passwords.

TABLE 4. Password setting trends.

Password Type	Number of Users	Avg. Password Length
Line-based passwords	97	10.62
Random characters only	28	8.74
Images only	9	6.71
Images and lines	14	9.82
Images and random characters	12	9.67

2) ACTIVITY TIMINGS

The registration and authentication timings for different type of passwords are given in Figure 10. The results show that the mean registration, easy login and secure login times of the proposed scheme are 20.84 seconds, 13.14 seconds, and 40.16 seconds, respectively. The results also show that users require less time for the secure login method when the passwords were created by means of drawings or lines. The reason for the lower time consumption is that all password elements in a line-based passwords are sequentially presented in the login screen. Highest time is required in secure login method when a password consists of random alphanumeric characters and images. More effort is required for searching the visibility of random alphanumeric characters inside the login screen, therefore authentication time increases in secure login method. Whereas, least time is required in easy login method when passwords consist of only alphanumeric characters, this is because the password characters can be quickly typed in the password field.

The secure login method sacrifices usability to gain a security advantage. Therefore, the easy login method is provided

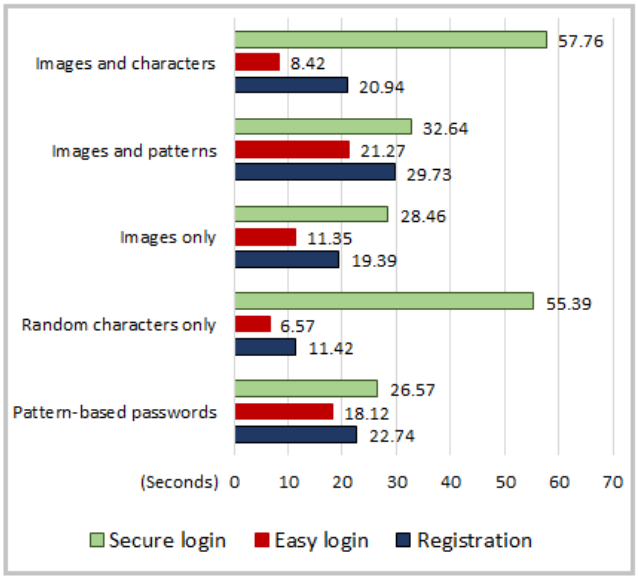


FIGURE 10. Password entry timings.

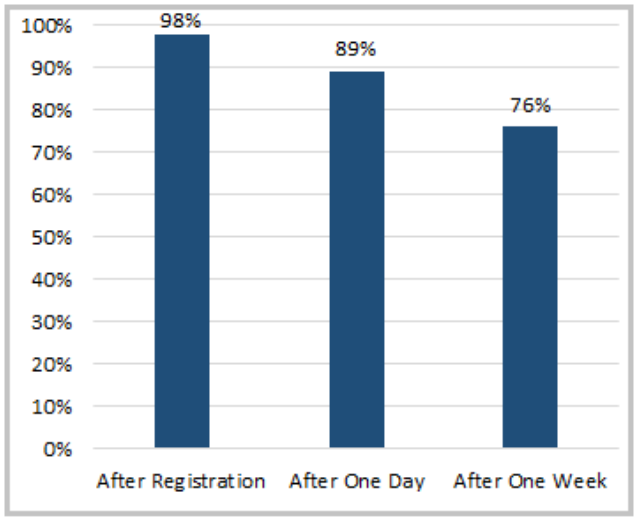


FIGURE 11. Password Memorability.

to improve the usability of the proposed scheme. The user can decide which method is more suitable based on the authentication environment and the type of application. Thus, the aspects of security and usability are balanced by providing two login methods.

VII. MEMORABILITY ANALYSIS

The proposed scheme provides visual cues for better memory recall of alphanumeric characters. The experimental results suggest that most of the users set passwords based on visual cues. The password memorability of the proposed scheme was tested through the testing application. It was analyzed immediately after registration, after one day and after one week. The users were asked to log in within three attempts. The memorability results were extracted from the log of the application developed for the experiment. In the log, both failed and successful login attempts by users were stored. The memorability (M) results were calculated by Equation (6).

$$M = \frac{U_s}{U_T} \tag{6}$$

where U_s is the number of users who were able to successfully log in, and U_T is the total number of users. In the first session of the password memorability tests, 160 users participated. In the second session, 6 participants were unavailable; therefore, the login activity was conducted by 154 registered users. In the third session, 19 participants were unavailable, so only 135 users performed the login activity. The results of the memorability tests are given in Figure 11.

The results suggest that 76% of the users remembered their passwords after one week. For textual password scheme, we have seen that 49% of the users remember their passwords over a time span of one week [19]. Users can set old textual passwords in the proposed scheme, therefore even higher percentage of password memorability can be achieved.

In textual password scheme, high-entropy passwords are difficult to memorize because they contain random combinations of alphanumeric characters. By contrast, high-entropy passwords are easier to remember in the proposed scheme due to the visual cues provided by password lines and pictures.

VIII. COMPARISON WITH OTHER AUTHENTICATION SCHEMES

A. RESILIENCE AGAINST SECURITY ATTACKS

We compare in this subsection our proposed scheme with other well-known authentication schemes against different security attacks; see Table 5. We measure the security of the schemes against a particular attack using a three-point rating system (Weak, Moderate, and Strong). The rating indicates the effort required to break a password using a particular attack. The grade of ''Strong'' indicates that a scheme requires a high level of effort to break the password and hence the scheme has a high level of resilience against a specific attack. The grade of ''Moderate'' indicates that the scheme has a medium level of resilience against a specific attack, while the grade of ''Weak'' indicates that the scheme has a low level of resilience against a specific attack.

The intensity or level of effort required to break a password against an attack for a particular scheme is found by comparing it with the traditional textual password scheme. If a scheme requires a level of effort similar to the traditional textual password scheme to break its password using a certain attack then we consider that the scheme is ''Weak'' against that particular attack. For example, in the textual password scheme, an attacker can break a password by recording a couple of login sessions; same is the case for the ColorLogin [15], PCCP [6], and GotPass [3] schemes, and the scheme by Lopez *et al.* [28]. Therefore, these schemes have received the ''Weak'' grade (see Table 5). Similarly, in contrast to the textual password scheme, a password dictionary is very difficult to create in PCCP [6], GOTPass [3], CHC [41], and CA [41]

TABLE 5. Comparison of Different Authentication Schemes against Various Security Attacks.

Scheme	Brute-Force	Dictionary	Shoulder Surfing	Key/Mouse Logger	Random Guessing	Multiple Recording	Phishing
Textual Password	Moderate	Weak	Moderate	Weak	Strong	Weak	Weak
Easy login	***Strong***	***Moderate***	***Moderate***	***Weak***	***Strong***	***Weak***	***Weak***
ColorLogin [15]	Moderate	Moderate	Weak	Strong	Strong	Weak	Moderate
PCCP [6]	Strong	Strong	Weak	Weak	Strong	Weak	Moderate
Lopez *et al.* [28]	Weak	Moderate	Strong	Strong	Moderate	Moderate	Strong
PPC [32]	Moderate	Weak	Strong	Strong	Strong	Moderate	Moderate
GotPass [3]	Strong	Strong	Weak	Strong	Strong	Weak	Moderate
CA [41]	Strong	Strong	Strong	Strong	Strong	Moderate	Moderate
CHC [43]	Strong	Strong	Strong	Moderate	Strong	Moderate	Strong
Secure login	***Strong***	***Strong***	***Strong***	***Strong***	***Moderate***	***Strong***	***Strong***

TABLE 6. Comparison of the Password Elements, Authentication Time, and Mean Resilience for Various Schemes.

Scheme	Password Elements	Mean Authentication Time (Seconds)	Mean Resilience
Textual Password	Alphanumeric	6.35	3.428
Easy login	***Alphanumeric, images***	***13.91***	***4.714***
ColorLogin [15]	Alphanumeric, colors	18	5.285
PCCP [6]	Click points	11 to 89	5.428
Lopez *et al.* [28]	Images of human faces	11.98	6.571
PPC [32]	Alphanumeric	47.3	6.571
GotPass [3]	Lines, images	24.5	6.714
CA [41]	Icons	> 120	8.571
CHC [43]	Icons	71.66	8.571
Secure login	***Alphanumeric, images***	***40.16***	***9.285***

schemes, and in the secure login method of our proposed scheme. Therefore, these schemes have been given the rating "Strong" against the dictionary attack (see Table 5). Note that the schemes are listed in the table based on their overall resilience in order of worst to best.

The ratings (Weak, Moderate and Strong) for the proposed scheme were determined from the security analyses given in Section V. The ratings for the rest of the schemes were extracted from the literature related to the schemes and by the security analyses of the respective schemes. For example, the CHC (Convex Hull Click) [43] scheme is "Strong" against the brute force attack because it provides one thousand icons for password creation.

B. AUTHENTICATION TIME AND MEAN RESILIENCE

Table 6 compares the type of password elements used by the various schemes (Column 2), the mean authentication time (Colum 3), and the mean resilience (Column 4) of the proposed scheme and other well-known schemes. The authentication time of the proposed scheme is determined from the usability analysis given in Section VI. The authentication time for the other schemes is extracted by the literature related to the schemes. The Mean Resilience is computed using Equation (7).

$$Mean\ Resilience = (\sum_{i \in K} r_i) \ / \ |K| \tag{7}$$

where K is the set of all security attacks and r_i is the resilience score or grade for a scheme against a particular attack in set K. To calculate Mean Resilience using Equation (7), we have used the set K comprising the seven attacks listed in Table 5. Note that it is possible to add additional attacks. The values of r_i are also derived from the three-point grading (Weak, Moderate, and Strong) given to various schemes in Table 5. We have assigned numerical scores 1, 5, and 10, to the three grades Weak, Moderate, and Strong, respectively. Note that assigning a different set of scores to the three grades (e.g., 1, 2, 3; or 2.5, 5, 10) will create similar *relative* scores for all the schemes. The schemes in Table 6 are listed in the order of lowest to highest Mean Resilience scores. A higher Mean Resilience score is better. Note in the table that the secure login method of our proposed scheme has the highest Mean Resilience (9.285) while the textual password scheme have the lowest Mean Resilience. The second best Mean Resilience score (8.571) is for the CA (Cognitive Authentication) [41] and CHC [43] schemes. The easy login method of our scheme has better Mean Resilience than the textual password scheme, however, most schemes have better Mean Resilience than the easy login method. See Section VIII-A for the explanation of the three-point grade scores that are used to compute Mean Resilience for the various schemes.

The lowest authentication time in Table 6 is for the textual password scheme (6.35 seconds) while the two highest authentication times are for the CA (Cognitive Authentication) [41] ($>$ 120 seconds) and CHC [43] schemes (71.66 seconds). The authentication time for the easy login method (13.91 seconds) is higher than the textual password scheme and a couple of other schemes. The reason for this is that the easy login method allows the use of images in the passwords and the utilization of drawing-based passwords. Four keys must be pressed to enter a picture, which increases the authentication time of the easy login method because

more work is required to enter a password element. The authentication time for the secure login method (40.16 seconds) is higher than some other schemes, however, it offers much better Mean Resilience than any of the other schemes. Based on the results in Table 6, we conclude that the secure login method provides the best overall performance.

The majority of the users who participated in the experiments related to our proposed scheme remembered only drawings instead of the individual password elements (see Section VI). As a result, these users had to search for the password elements on the login screen before typing their passwords. The search for password elements will typically increase the overall mean authentication time for any scheme. For example, we found that the authentication time of the easy login method for the users who completely remembered their alphanumeric passwords (i.e., they did not need to search) was the same as in a textual password scheme.

Our experiments, which were used to calculate these authentication times only involved one registration session and three authentication trials. A total of three trials do not give sufficient practice to improve authentication speeds for a new scheme. We believe that the authentication times will significantly improve with further practice and adoption of the scheme by people. Moreover, better login screen layouts and improved implementations of the scheme will also reduce the authentication time and improve its usability and adoption.

C. MULTI-FACTOR AUTHENTICATION SCHEMES

Multi-factor authentication techniques have many security advantages but they also come with some usability and security weaknesses [39]. For example, these techniques may require uninterrupted cellular or internet service when the authentication information is received through email or SMS. Some multi-factor authentication schemes require additional hardware for authentication such as a mobile phone or a smart card [18], [25]. In these cases the users should always keep the extra hardware with them or otherwise, they will not be authenticated to a system. Some of these techniques also inherit security weaknesses because the schemes use a human-readable or plain text format for authentication-related information. For example, SMS-based authentication information can be recorded and sent to hackers by different applications installed on a smartphone. Similarly, after hacking a user's email account the authentication information can be captured.

The use of the secure login method in the proposed scheme offers benefits of the OTP approaches while avoiding usability and security issues of multi-factor authentication techniques. A user does not need to receive a password from any third-party source but it is calculated from the secure login screen, and therefore the passwords cannot be recorded. The proposed scheme is also efficient to use because it does not require any additional hardware for authentication.

Some authentication schemes such as the scheme proposed by Lopez *et al.* [28] generate a password based on some calculations. However, the usability disadvantage of this [28] scheme is that the authors use a completely new login process and set of elements for password creation. In the proposed scheme, the traditional textual password elements are augmented with pictures to allow users to easily switch towards the proposed scheme.

D. EAVESDROPPING

Due to the broadcast nature of communication, wireless networks are vulnerable to eavesdropping [13]. A common approach for avoiding eavesdroppers to gain access to confidential information is to transmit encrypted data. In the secure login method of the proposed scheme, temporary numbers pass through the communication network instead of an actual password. Therefore, eavesdroppers cannot get an actual password from the communication network. However, in the case of the easy login method, the communication network should be secured through some protocols such as SSL [14] because the actual passwords cross through the networks. These two cases apply to all the schemes with respective requirements.

E. CACHING

Caching could be used to increase the speed of content loading [35]. Different techniques are used to cache the information [44]. Some authentication techniques have developed specific methods to improve caching performance, such as in [26], frequently used information is stored in cache-enabled nodes to reduce data processing and information loading time for the login process. Authentication pages are frequently used and are generally cached to improve performance. In the proposed scheme, the login pages will not benefit from caching because new pages are generated at each of the three steps of the login process with 50% randomly selected new elements. Therefore, the secure login method and other similar schemes where pages are randomly generated could have disadvantages in terms of caching performance. These performance issues related to such schemes could be addressed by developing new caching strategies.

IX. CONCLUSION AND FUTURE WORK

Despite security issues, textual password schemes have been used for user authentication for many decades. A large number of graphical password schemes have been proposed but none has fully replaced textual passwords. In both textual and graphical password schemes, easy-to-remember passwords are easy to break, while secure or strong passwords are difficult to remember. Both types of authentication schemes are susceptible to multiple recording attacks. Usability is another problem with relatively secure graphical password schemes because these schemes require long login time and more effort for authentication. Various hybrid schemes have been proposed over the years to address the challenges of textual and graphical passwords. However, these schemes remain vulnerable to various attacks, could be affected due to multiple recording attacks, while some hybrid schemes

requiring additional hardware for password entry, affecting their usability.

In this paper, we have proposed a textual-graphical hybrid authentication scheme that improves the security, memorability and usability inadequacies of existing authentication schemes. The proposed scheme provides two different methods of entering the password — the easy login method and the secure login method — and thereby provides a trade-off between security, memorability, and usability. The user could dynamically switch to any of these methods based on the security of the surrounding environment or the criticality of the user account. The easy login method is similar to the traditional login methods except that users could select alphanumeric characters and/or pictures for their passwords and use shortcut keyboard keys to enter passwords. The secure login method leverages a three-step procedure along with a simple calculation involving a random selection of the password elements and the numerical values assigned to the password elements. Moreover, the provided visual cues help users to easily memorize strong alphanumeric passwords and improve the memorability and usability property of the scheme. The scheme does not require additional hardware and therefore provides better usability.

We have implemented and analysed the proposed scheme for its security against seven different security attacks. We have also investigated its usability and memorability, reporting various trends of password elements used and the respective authentication times. Moreover, we have compared the proposed scheme with eight other well-known password-based authentication schemes in terms of its resilience and authentication time. The results and analyses have demonstrated the effectiveness of the proposed scheme. We have not attempted in this paper to provide formal proof of the security properties of the proposed scheme and rather to analyse it empirically and using descriptive analysis. A number of works published in good journals have reported empirical or simulation-based analysis of their proposed schemes and have not formally proved the security properties of their schemes. For example, Dongdong and Wenjian [46] used only a descriptive analysis to evaluate their proposed scheme. In the security analysis, they targeted four attacks (replay, guessing, exhaustive, and man-in-the-middle attacks). Alsaiari *et al.* [3] used simulations to evaluate their proposed scheme against guessing, intersection, and shoulder-surfing attacks. Wazid *et al.* [40] analysed their scheme using empirical analysis against eight types of attacks; replay, man-in-the-middle, privileged-insider, user impersonation, smart meter impersonation, ephemeral secret leakage, password change, anonymity, and untraceability attacks. Yu *et al.* [45] also evaluated their proposed scheme using empirical analysis against seven types of attacks; shoulder-surfing, exhaustive, dictionary, social engineering, smudge, images-harvest, and technology-based recording attacks. Ali *et al.* [2] evaluated their proposed scheme using different algorithms that they devised themselves against brute force and shoulder surfing attacks to show improvements in the client and server-side security. Our future work will look also into formal methods for the analysis of this proposed scheme.

The proposed scheme includes 118 password elements, 94 of these are alphanumeric characters and the remaining 24 elements are pictures. A user can set a password with elements from the set of all 118 password elements. We describe in this paper one possible implementation of the proposed authentication scheme. Other implementations are also possible, such as with two or more than three steps to enter the password in the secure login method, with different registration and login screens, different ways of placements of pictures and alphanumeric keys in a single page, a different number or kinds of pictures for password entry, the categories of pictures, etc. We have shown in the paper three different ways of placing the pictures on the login screen (see Figures 2, 7, and 8). It is possible for the developers to provide an implementation of the scheme where the set of pictures, symbols, and alphanumeric elements can be selected or defined by the users. However, this could create risks of predictability and guessability in identifying user passwords. This is an area where further research is needed and could produce fruitful results.

Password memorability is degraded for high-entropy passwords. In the proposed scheme, this issue of providing both high memorability and entropy is addressed using a pattern or drawing-based approach for setting up the password by selecting alphanumeric characters and images. By representing alphanumeric characters and images in a certain visual pattern — such as a snake made with straight lines, a multi-digit number (e.g., the number "11" shown in Figure 3), etc. — the login screen of the proposed scheme assists users in easily remembering random alphanumeric characters and images. See the explanation in Section V-A1. Traditional textual password dictionaries are not effective when passwords are created from visual patterns. However, research is required about the patterns users mostly draw for password creation. Similar password patterns allow attackers to create password dictionaries. The proposed scheme with a mix of alphanumeric and image password elements and a range of security mechanisms facilitates a very rich space for setting complex passwords and it is only limited by the imagination of the user. The user selection of a complex visual pattern, however, could increase the password authentication time. In our view, this is up to the user to find a balance for herself between memorability, usability, and security. Using our scheme, a user may consider a longer authentication time associated with a complex visual pattern agreeable considering the fact that OTP-based passwords are being widely used these days and they typically take longer than the times required by our scheme due to the absence of third-party services. Sometimes these third-party services do fail and in other times these services may take a few minutes or more. Setting up a password using a complex but personalised, easy-to-remember pattern by an individual is a convention and practice that once adopted by people will become easier for everyone and will open new doors for

developing high-security passwords. We will investigate and compare these aspects of the scheme in the future and we also call on the community for the same.

Note that the reason we refer to the scheme as a hybrid textual-graphical scheme is to highlight that it uses both textual and graphical password elements. This hybrid textual-graphical aspect (that does improve the entropy of the password due to its resilience against dictionary, brute force, etc. attacks) alone does not describe the novelty of the scheme rather, as explained earlier, the several novel mechanisms used in the scheme and their novel combination represent the novelty of the scheme. Commenting further on the adoption of hybrid textual-graphical passwords by users, we believe that the reason for the wide use of one type of passwords (where a choice to select a password with one type of elements is given) is due to the norm that most people use alphanumeric passwords in their daily routines. This behaviour can be intervened by highlighting the security benefits of hybrid elements in the passwords, providing incentives, or setting mandatory mixed-password policies. These issues need to be investigated in the future.

We believe that the authentication times of our proposed will significantly improve with further practice and adoption of the scheme by people. Our experiments, which were used to calculate authentication times only involved one registration session and three authentication trials. A total of three trials do not give sufficient practice to improve authentication speeds for a new scheme. Moreover, better login screen layouts and improved implementations of the scheme will also reduce the authentication time and improve its usability and adoption.

Future work will investigate and improve the proposed scheme further in terms of its security, usability, and memorability.

REFERENCES

[1] (2019). *John the Ripper Password Cracker*. Accessed: Jul. 3, 2019. [Online]. Available: http://www.openwall.com/john/

[2] M. Ali, A. Baloch, A. Waheed, M. Zareei, R. Manzoor, H. Sajid, and F. Alanazi, "A simple and secure reformation-based password scheme," *IEEE Access*, vol. 9, pp. 11655–11674, 2021.

[3] H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell, "Graphical one-time password (GOTPass): A usability evaluation," *Inf. Secur. J., Global Perspective*, vol. 25, nos. 1–3, pp. 94–108, Apr. 2016.

[4] G. E. Blonder, "Graphical password," U.S. Patent 5 559 961, Sep. 24, 1996.

[5] N. Chakraborty and S. Mondal, "Color pass: An intelligent user interface to resist shoulder surfing attack," in *Proc. IEEE Students' Technol. Symp.*, Feb. 2014, pp. 13–18.

[6] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. Van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 222–235, Mar. 2012.

[7] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Computer Security—ESORICS 2007*. Berlin, Germany: Springer, 2007, pp. 359–374.

[8] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proc. 13th Conf. USENIX Secur. Symp.*, vol. 13, 2004, p. 11.

[9] R. Dhamija and A. Perrig, "Deja Vu—A user study: Using images for authentication," in *Proc. USENIX Secur. Symp.*, vol. 9, 2000, p. 4.

[10] P. Dunphy, *Usable, Secure and Deployable Graphical Passwords*. School of Computing Science, Newcastle University, 2013.

[11] P. Dunphy, J. Nicholson, and P. Olivier, "Securing passfaces for description," in *Proc. 4th Symp. Usable privacy Secur. (SOUPS)*, 2008, pp. 24–35.

[12] P. Dunphy and J. Yan, "Do background images improve 'draw a secret' graphical passwords?" in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 36–47.

[13] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7599–7603, Aug. 2017.

[14] A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (SSL) protocol version 3.0," Netscape Commun. Corp., Mountain View, CA, USA, 2011.

[15] H. Gao, X. Liu, R. Dai, S. Wang, and X. Chang, "Analysis and evaluation of the ColorLogin graphical password scheme," in *Proc. 5th Int. Conf. Image Graph.*, Sep. 2009, pp. 722–727.

[16] GeneratePasswords.org. (2019). *How to Calculate Password Entropy*. Accessed: Mar. 2, 2019. [Online]. Available: https://generatepasswords.org/how-to-calculate-entropy/

[17] J. Gosney, "Password cracking HPC," in *Proc. Passwords Conf.*, 2012, pp. 6–34.

[18] W. A. Hammood, R. Abdullah, O. A. Hammood, S. M. Asmara, M. A. Al-Sharafi, and A. M. Hasan, "A review of user authentication model for online banking system based on mobile IMEI number," in *Proc. IOP Conf. Ser., Mater. Sci. Eng.*, 2020, vol. 769, no. 1, pp. 1–10.

[19] S. M. T. Haque, "Human factors in textual password-based authentication," Univ. Texas Arlington, Arlington, TX, USA, 2015.

[20] J. Hendryli and D. E. Herwindiati, "Voice authentication model for one-time password using deep learning models," in *Proc. 2nd Int. Conf. Big Data Eng. Technol.*, 2020, pp. 35–39.

[21] J. Iftikhar, S. Hussain, K. Mansoor, Z. Ali, and S. A. Chaudhry, "Symmetric-key multi-factor biometric authentication scheme," in *Proc. 2nd Int. Conf. Commun., Comput. Digit. Syst. (C-CODE)*, Mar. 2019, pp. 288–292.

[22] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proc. USENIX Secur.*, 1999, pp. 1–15.

[23] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[24] T. Kansuwan and T. Chomsiri, "Authentication model using the bundled CAPTCHA OTP instead of traditional password," in *Proc. Joint Int. Conf. Digit. Arts, Media Technol. ECTI Northern Sect. Conf. Electr., Electron., Comput. Telecommun. Eng. (ECTI DAMT-NCON)*, Jan. 2019, pp. 5–8.

[25] A. Kumari, S. Jangirala, M. Y. Abbasi, V. Kumar, and M. Alam, "ESEAP: ECC based secure and efficient mutual authentication protocol using smart card," *J. Inf. Secur. Appl.*, vol. 51, pp. 1–12, Apr. 2020.

[26] X. Lai, J. Xia, M. Tang, H. Zhang, and J. Zhao, "Cache-aided multiuser cognitive relay networks with outdated channel state information," *IEEE Access*, vol. 6, pp. 21879–21887, 2018.

[27] M.-K. Lee, H. Nam, and D. K. Kim, "Secure bimodal PIN-entry method using audio signals," *Comput. Secur.*, vol. 56, pp. 140–150, Feb. 2016.

[28] N. Lopez, M. Rodriguez, C. Fellegi, D. Long, and T. Schwarz, "Even or odd: A simple graphical authentication system," *IEEE Latin Amer. Trans.*, vol. 13, no. 3, pp. 804–809, Mar. 2015.

[29] Y. Meng, "Designing click-draw based graphical password scheme for better authentication," in *Proc. IEEE 7th Int. Conf. Netw., Archit., Storage*, Jun. 2012, pp. 39–48.

[30] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, p. 1, Jan. 2018.

[31] H.-T. Pan, H.-W. Yang, and M.-S. Hwang, "An enhanced secure smart card-based password authentication scheme," *IJ Netw. Secur.*, vol. 22, no. 2, pp. 358–363, 2020.

[32] K. Rao and S. Yalamanchili, "Novel shoulder-surfing resistant authentication schemes using text-graphical passwords," *Int. J. Inf. Netw. Secur.*, vol. 1, no. 3, p. 163, Jul. 2012.

[33] R. R. Schaller, "Moore's law: Past, present and future," *IEEE Spectr.*, vol. 34, no. 6, pp. 52–59, Jun. 1997.

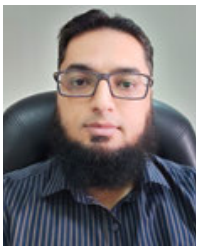
[34] E. M. Scheidt and E. Domangue, "Multiple factor-based user identification and authentication," U.S. Patent US 6 845 453 B2, Jan. 18, 2005.

[35] F. Shi, L. Fan, X. Liu, Z. Na, and Y. Liu, "Probabilistic caching placement in the presence of multiple eavesdroppers," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–10, May 2018.

[36] U. V. Sorochi, A. Nasiru, and I. A. Inusa, "Security enhancement for building access, using one time password (OTP) technology," *Eur. J. Electr. Eng. Comput. Sci.*, vol. 4, no. 3, pp. 1–9, Jun. 2020.
[37] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in *Proc. USENIX Secur.*, vol. 7, 2007, pp. 1–8.
[38] C. Varenhorst, M. V. Kleek, and L. Rudolph, "Passdoodles: A lightweight authentication method," Res. Sci. Inst., 2004, pp. 1–11.
[39] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101619.
[40] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for renewable-energy-based smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3144–3153, Dec. 2017.
[41] D. Weinshall, "Cognitive authentication schemes safe against spyware," in *Proc. IEEE Symp. Secur. Privacy (S P)*, Dec. 2006, p. 6.
[42] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. Hum.-Comput. Stud.*, vol. 63, nos. 1–2, pp. 102–127, Jul. 2005.
[43] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proc. Work. Conf. Adv. Vis. Interfaces (AVI)*, 2006, pp. 177–184.
[44] J. Xia, F. Zhou, X. Lai, H. Zhang, H. Chen, Q. Yang, X. Liu, and J. Zhao, "Cache aided Decode-and-Forward relaying networks: From the spatial view," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–9, Apr. 2018.
[45] X. Yu, Z. Wang, Y. Li, L. Li, W. T. Zhu, and L. Song, "EvoPass: Evolvable graphical password against shoulder-surfing attacks," *Comput. Secur.*, vol. 70, pp. 179–198, Sep. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016740481730113X
[46] D. Zhao and W. Luo, "One-time password authentication scheme based on the negative database," *Eng. Appl. Artif. Intell.*, vol. 62, pp. 396–404, Jun. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0952197616302251
[47] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops (AINAW)*, vol. 2, 2007, pp. 467–472.
[48] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A hybrid password authentication scheme based on shape and text," *J. Comput.*, vol. 5, no. 5, pp. 765–772, May 2010.

SHAH ZAMAN NIZAMANI received the Ph.D. degree in user authentication from the Quaid-e-Awam University of Engineering Science and Technology. He is currently working as an Associate Professor with the Department of Information Technology, Quaid-e-Awam University of Engineering Science and Technology. Previously, he has six years of software development experience. His research interests include information security, algorithm complexity, and software estimation.

SYED RAHEEL HASSAN received the Ph.D. degree in network security from the Universite de Franche-Comte, France. Before his Ph.D., he worked few years in the industry as a Network Administrator. He has been working in academia for last seven years and published several articles. In past, he has completed a Research Fellowship at Emory University, USA. He is currently with the Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, which is ranked 186 according to QS world ranking of the universities for 2019. He is involved in multiple projects related to Network Security, such as Intrusion Detection Systems in distributed networks and Smart Authentication for future networks.



RIAZ AHMED SHAIKH received the Ph.D. degree from the Computer Engineering Department, Kyung Hee University, South Korea, in 2009. He is currently an Associate Professor with the Computer Science Department, King Abdulaziz University, Jeddah, Saudi Arabia. He wrote more than 50 research articles published in peer-reviewed journals and conferences. The two U.S. and one Korean patents are issued to him. His research interests include privacy, security, trust management, risk estimation, sensor networks, vehicular networks, and the IoT. He has served as a technical program committee member for more than 35 international conferences. He was also an Editor of the book entitled *Secure Cyber-Physical Systems for Smart Cities* (USA: IGI Global).

EHAB ATIF ABOZINADAH received the graduate degrees from the Engineering School, George Mason University, USA, the master's degree in information technology, the master's degree in information systems, and the Ph.D. degree in smart cybersecurity. He received the two graduate certificate degrees in information security and e-commerce. He is currently an Assistant Professor with the Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University (KAU), Jeddah, Saudi Arabia. He is also the Vice Dean of Development at e-Learning Deanship and the Director of the High Performance Computing (HPC) Center, KAU. He is supervising the AI program aimed at offering an AI curriculum for all the undergraduate programs with KAU. Also, he is participating in the smart e-learning research team at KAU that focuses on the usability of the massive e-learning data that includes the learning styles, student behaviours, and measurable learning outcomes on building smart e-learning systems. In addition, he is supporting AI research groups to recognize the benefits of HPC systems on speeding up the data processing of AI models. Also, he is working in many research strands that focus on artificial intelligence, such as cybersecurity and social media mining for building smart detection systems that identify cyber-criminal accounts to improve the security of social media. Specializations: cybersecurity, artificial intelligence, big data, social media mining, and data science.

RASHID MEHMOOD (Senior Member, IEEE) is currently the Research Professor of Big Data Systems and the Director of Research, Training, and Consultancy with the High Performance Computing Centre, King Abdulaziz University, Saudi Arabia. He has gained qualifications and work experience from universities in the U.K., including Cambridge and Oxford Universities. He has 25 years of academic and industrial experience in computational modelling, simulations, and design using computational intelligence, big data, high performance computing, and distributed systems. His broad research aim is to develop multi-disciplinary science and technology to enable a better quality of life and smart economy with a focus on real-time intelligence and dynamic (autonomic) system management. He has published nearly 200 research articles, including six edited books. He has organised and chaired international conferences and workshops, including EuropeComm 2009, Nets4Cars 2010–2013, SCE 2017–2019, SCITA 2017, and HPC Saudi 2018–2020. He has led and contributed to academia-industry collaborative projects funded by EPSRC, EU, U.K. regional funds, and Technology Strategy Board U.K. with the value of over $50 million. He is also a Founding Member of the Future Cities and Community Resilience (FCCR) Network, a member of ACM and OSA, and the former Vice-Chairman of *IET Wales SW Network*.