A Novel Hybrid Password Authentication Scheme Based on Text and Image

Ian Mackie, Merve Yildirim

A Novel Hybrid Password Authentication Scheme Based on Text and Image

I. Mackie and M. Yıldırım

Department of Informatics
University of Sussex
Brighton, UK
i.mackie@sussex.ac.uk

Abstract. Considering the popularity and wide deployment of text passwords, we predict that they will be used as a prevalent authentication mechanism for many years to come. Thus, we have carried out studies on mechanisms to enhance text passwords. These studies suggest that password space and memorability should be improved, with an additional mechanism based on images. The combination of text and images increases resistance to some password attacks, such as brute force and observing attacks. We propose a hybrid authentication scheme integrating text and recognition-based graphical passwords. This authentication scheme can reduce the phishing attacks because if users are deceived to share their key passwords, there is still a chance to save the complete password as attackers do not know the users' image preferences. In addition to the security aspect, the proposed authentication scheme increases memorability as it does not require users to remember long and complex passwords. Thus, with the proposed scheme users will be able to create strong passwords without sacrificing usability. The hybrid scheme also offers an enjoyable sign-in/log-in experience to users.

Keywords: Passwords, authentication, recognition based graphical passwords.

1 Introduction

User authentication is one of the most important parts of the security of information systems. The most common approach for authenticating human users is text passwords. Evidence shows that users generally choose weak passwords so that they can remember them easily [1, 21]. This increases the possibility of the passwords being cracked. When users are requested to create long and complex passwords, they resort to coping strategies such as writing passwords down or reusing them [4]. Therefore, text-based passwords suffer from a whole variety of drawbacks such as vulnerabilities to dictionary attacks, brute force attacks and social engineering.

Graphical passwords are considered a good replacement for textual passwords. The fact that humans can recognize and remember images easier than

text can be a solution to the memorability problem [16]. However, they are more vulnerable to shoulder surfing attacks as compared to textual passwords. Also, the graphical password authentication is relatively expensive to implement which prevents it becoming widespread. To overcome the weaknesses of text and graphical passwords, this paper introduces a hybrid authentication scheme which is a combined approach of text and graphical passwords.

2 Background and Related Work

Many hybrid authentication schemes have been proposed in recent years to overcome the drawbacks of knowledge based authentication schemes. While some researchers integrated different types of graphical passwords [10], others combined graphical passwords with text passwords [12, 14, 17]. These researchers proposed solutions to shoulder surfing attacks to strengthen the graphical password schemes. Rao and Yalamanchili [14] proposed two authentication schemes using graphical passwords called Pair Pass Char (PPC) and Tricolor Pair Pass Char (TPPC). Both these schemes support two modes of input: keyboard entry and mouse clicks. The first mode is the text mode and the other one is the graphical mode. Rao and Yalamanchili carried out an experiment with 20 graduate students and found that the average login times increase as the password length increases in both schemes. The study also showed that the login times for TPPC scheme is higher, and rules for this scheme are more difficult to be applied. The PPC scheme provides passwords similar to that offered by conventional password systems, and it is greatly enhanced in the TPPC scheme as it uses the same character set in three colours. The login times increase where the password space is enhanced in these proposed schemes, and thus usability is sacrificed for security.

Zhao and Li [23] proposed S3PAS which is a scalable shoulder-surfing resistant password authentication scheme. S3PAS is designed for client/server environments. It integrates both graphical and textual password schemes and aims to provide resistance to shoulder surfing, hidden camera and spyware attacks. In this scheme two kinds of password are generated: original passwords and session passwords. Users create original passwords when they create their accounts and input different session passwords in every login process to protect their original passwords. There are some drawbacks in this system similar to other text based graphical password schemes. S3PAS schemes include complicated and longer login processes.

In another study, two authentication techniques based on text and colours are proposed [17]. These techniques are called pair-based authentication scheme and hybrid textual authentication scheme which are suitable for Personal Digital Assistants (PDAs). Both techniques use a grid for session passwords generation. The researchers claim that these schemes are resistant to shoulder-surfing, dictionary and brute force attacks. However, they did not conduct a detailed user study to evaluate the security of the schemes. They only measured the registration and login times of the passwords created with these schemes by 10 partic-

ipants. Since these schemes are completely new to the users and there is not a proper security and usability analysis of them, these proposed techniques should be verified extensively for security usability and effectiveness in the future. Similarly, there is not any user study conducted to test the security and usability of another text-based shoulder surfing resistant graphical scheme proposed by Chen et al. [5].

Zhang et al. [22] also proposed a hybrid password scheme based on shape and text. The proposed scheme uses shapes of strokes as origin passwords and allows users to login with text passwords via traditional input devices. Although the researchers claim that the scheme is resistant to shoulder surfing, hidden camera and brute force attacks and that it has variants to strengthens the security level through changing login interface of the system, the scheme still has some security and usability drawbacks. It is not familiar to users so they may adopt simple and weak strokes. This increases the chance of attackers to obtain the passwords. Also, the password creating step is vulnerable to attacks since users have to tell the system the original shapes and strokes. Moreover, the login process of this scheme is longer than other graphical schemes. For these reasons, more advanced authentication system should be proposed to improve this method.

In a recent study, a comprehensive survey on shoulder surfing resistant text based graphical password schemes is conducted [12]. This study explained the existing security problems, possible solutions and limitations of some of these schemes. These studies primarily focused on the existing shoulder surfing attacks in text based graphical password approach. However, a guessing attack is also a potential problem for graphical password schemes because of the predictability of user-chosen graphical passwords [18, 20].

3 The Novel Authentication Scheme

All the aforementioned schemes have discrete text and graphical password creation steps which considerably increase the registration and login times. Compared to these schemes, the novel hybrid authentication scheme introduced in this research shortens password creation and login times as it has an integrated registration phase. Unlike other schemes, in the proposed scheme, images are used as cues to help users to complete their complex text passwords instead of creating a second password. Thus, the proposed scheme improves recall rate without sacrificing the security against attackers. Moreover, the results of the previous studies showed that users have an adoptability problem with these schemes as they are unfamiliar to users. However, the proposed scheme substantially preserves the login experiences of users who are accustomed to traditional textual passwords. As far as is known, the proposed scheme is the first scheme in the literature associating the letters of the chosen text passwords with the images by using the Tip of the Tongue (TOT) phenomenon. This feature significantly increases the memorability of the passwords.

In the hybrid authentication method we propose, text passwords are strengthened by using images as an assistant tool for users to memorize complex char-

acter sets. Theoretically, it is a text password scheme integrating user chosen and system generated characters. However, users are allowed to choose images from image portfolios to enter the system generated characters associated with the images. In this approach, users continue to use text passwords, but strong and memorable ones. They do not have to remember complex passwords at first or write them down; with the help of the images they will be able to memorize them naturally.

The proposed scheme has many advantages in terms of security and usability. It allows users to create and memorize cryptographically strong passwords easily. It eliminates the risk of passwords being hacked by dictionary attacks. It also secures the passwords against shoulder surfing attacks. It is a user-friendly authentication scheme.

The next sections describe the proposed scheme in detail considering its design and security and usability aspects.

3.1 System Design

To test the proposed authentication scheme, a web application which also works on mobile phones has been designed and implemented. This application uses ASP as the server side programming, JavaScript as the client side programming, and an SQL database is used to store the data.

The user authentication process in the designed scheme has two main steps: a registration phase and a login phase. The registration phase consists of creating key passwords and image selection. The reasons behind key design decisions and how they relate to security and usability considerations are explained at every stage of the registration and login phases in the following sections. The flowcharts of the registration and login phases are illustrated in Figure 1.

Registration Phase. In the first step of the registration phase, users are asked to enter their username or email address in the username field. Then they are asked to create a key text password called key characters. The only restriction about the key password is that the first four characters should be upper- or lower-case characters. The reason why the minimum length of key password is set to four characters is that every user can remember it easily.

After creating the key password, the image selection process begins. This is an integrated process of retyping the key password and choosing the images. While users retype their key passwords in the "password" field, an associated image portfolio appears each time they type a particular letter. For each typed letter, there is a related image portfolio consisting of 20 images. This relation comes from the idea of choosing images of objects, famous people, activities or known figures which their names initials is the typed letter. It means, for example, when users type "a", as a character in their key passwords, an image portfolio appears including images whose names are starting with "a" (the images of alpha, apple, Albert Einstein etc.). Then users select the images from the image portfolio. Users have to select an image from each set of images. This selection will be

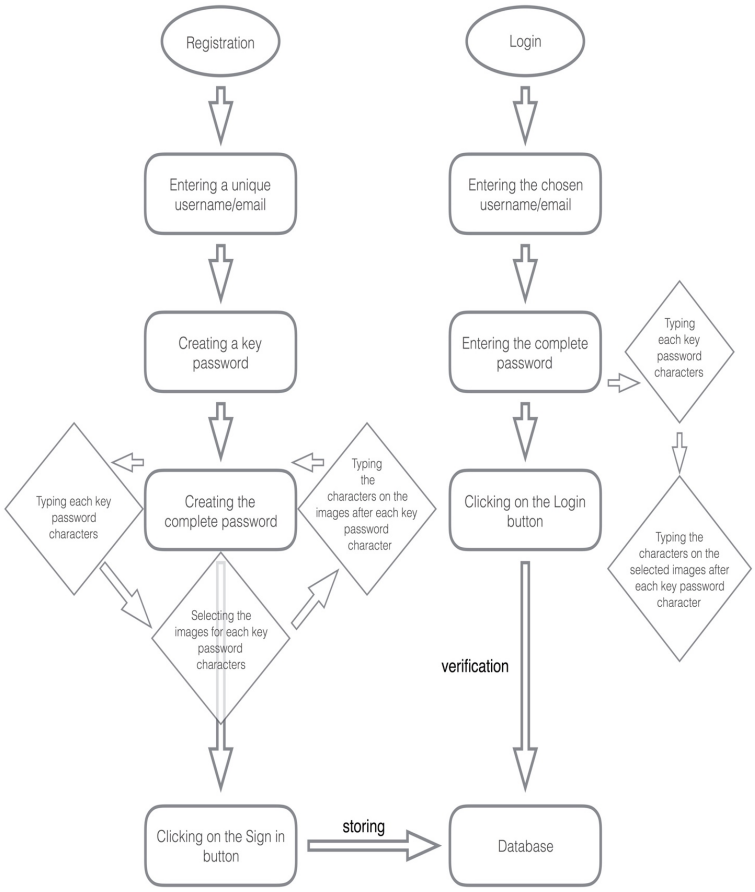


Fig. 1. The flowchart of registration and login phases.

performed so as users type the characters under the images into the password field but not click on the image. There are a set of two random characters under each image combining one alphanumerical character and one digit or letter. Briefly, users will enter these two-characters after each character of their key password. To make it easy for users to recognize which characters they should enter, the password field is designed to include small and large squares. The small squares coloured in green is to enter each character of key passwords, and the larger squares coloured in red is to enter the characters under the images. This helps users not to be confused of the order of the characters. In this study, users are expected to choose four images in total which are associated to four letters in their key password, considering the memorability issues. Therefore, there are four small green squares for the first four alphabetical characters of the key password. Also, there are four larger red squares for the two sets of characters placed under the images. The last large square is to enter the rest of the key password's characters.

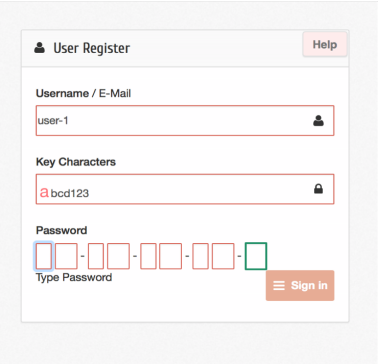
The number of images in each portfolio is set for the first test of the scheme. The theoretical password space calculated in this way have satisfying results to provide high security.

This progress allows users to create a complex password mixing their key passwords and the random characters associated with the selected images. The characters under each image change for different users. The registration phase of the scheme is illustrated in the Figure 2 (a-e) step by step with the example username, `user-1`, and the password, `abcd123`.

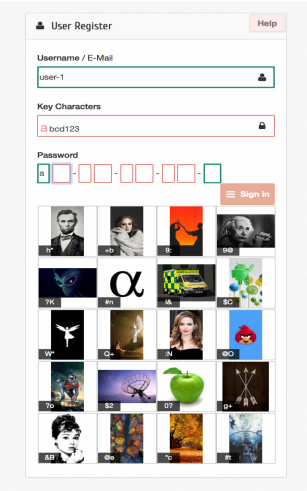
As seen in the figures, the password `abcd123` which is created as the key password by the user whose username is `user-1` turned into a complex password `ah*b-pcJ:d&x123` including upper case, lower case, number and special keyboard characters at the end of the experiment. The user chose the images of Abraham Lincoln, bag, cake and yellow dress and entered the characters under those images. The user does not have to remember the complex, 15 characters long password as remembering the key password and the four images will suffice. Even if users create four character password composed of only lower case characters, it will turn into a complex password including different type of characters when the password creation process ends.

The proposed scheme has a help feature which visualize the password creation instructions for users step by step. When the creation of a mixed password is completed, the sign up button becomes active to so that users can complete the registration process. All the details including username and complete passwords entered in the registration phase are stored into the database which will be used during the login phase for verification.

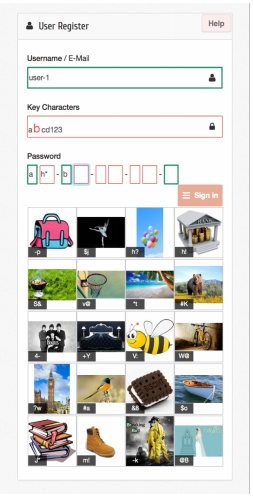
Login Phase. In the login phase users are asked to enter their user name/email and their passwords (mixed password). Users will be able to see the images like in the registration phase but the order of images within the set will be random at every login time. After a while as users continue to login the system, they will be able to memorize their complex passwords so they might not need to



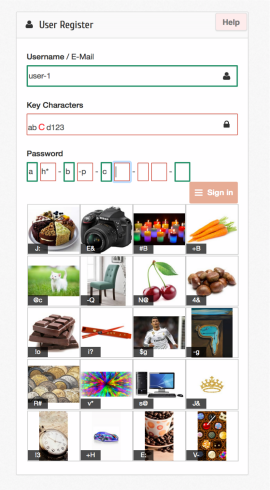
(a) Entering the username and the key password (key characters).



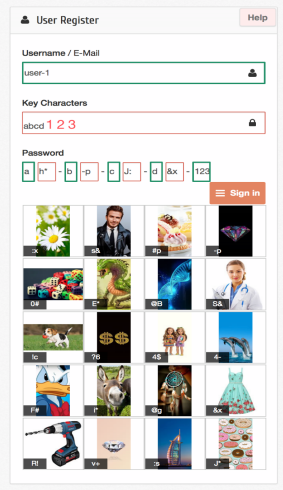
(b) Entering the first character of the key password and characters under the selected image from the portfolio.



(c) Entering the second character of the key password and characters under the selected image from the portfolio.



(d) Entering the third character of the key password and characters under the selected image from the portfolio.



(e) Entering the fourth character of the key password, characters under the selected image from the portfolio and rest of the characters of the key password.

Fig. 2. (a-e) User registration phase of the proposed scheme.

look at the images. The system has a feature which allows users to hide pictures whenever they want; this decreases the susceptibility shoulder surfing attacks. In case they have difficulties to recall the part of their passwords, they can view the images by simply ticking the "invisible pictures" box. The screen-shot of the login phase of the authentication scheme is shown in Figure 3.

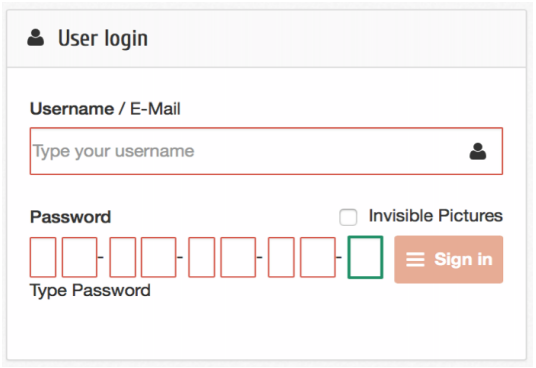


Fig. 3. User login phase of the proposed scheme.

In the login phase, while supplying the username/email and password information, independent of whether or not they match those defined during password creation, the image portfolios will continue to appear based on the typed character. Users must correctly enter the characters under all images pre-chosen for their accounts in each round of password verification. If any information is wrong, the user will be shown a "access denied" message at the end of the login phase. Seeing an image portfolio including no familiar image allows legitimate users to immediately realize that they entered a different character from key passwords characters and gives them chance to fix it. However, this prevents an attacker from knowing that the characters tried are invalid.

After the successful entries of both username/email and password, the users are allowed to access their accounts.

3.2 Security and Usability Analysis

The following sections presents the security and usability analysis of the proposed scheme. The password space of the scheme is formulated and its resistance to attacks is discussed under the security analysis. Password creation, login time and memorability of the passwords created with the scheme are discussed under the usability analysis.

Security Analysis. A new password scheme should allow users to create passwords which are strong enough against guessing, brute-force and observation

attacks. The quality of a password authentication scheme depends on how it is effective to limit attempts to guess users' passwords either by people who know them or a computer-based cracking program trying the possible passwords [11, 10]. Password strength is determined by measuring the password space which is the maximum possible number of passwords generated by the system. The password space of the novel authentication scheme is formulated in the following section.

Password Space. The strength of the proposed scheme can be evaluated by measuring both the entropy of the user chosen key-text password and the graphical password parts. Assume that the password space of the key password created by the users in our scheme is P_1, the length of the key password is l and n is the numbers of the characters in an alphabet from which the key passwords characters are randomly selected such as an alphabet including English upper and lower letters, digits and non-alphanumeric characters. The key password which is l characters long has an entropy of $l \cdot \log_2 n$ bits. In our scheme, however, this should be somewhat lower than this since at least four letters of the key password must be either upper or lower case so we calculate the password space of the key password in two parts. The password space for the key password is:

$$P_1 = (l-4) \cdot \log_2 n_1 \cdot 4 \cdot \log_2 n_2$$

To find the total password space, we also calculate the entropy of image based passwords. Let P_2 be the password space of image based passwords, and c be the number of rounds of choosing images from the related portfolios which is 4 in our case since at least 4 different images should be chosen from different portfolios. Assume that n is the numbers of images in each portfolio, and k is the number of images selected from each portfolio. The entropy of a randomly selected images and accordingly the two-character sets is:

$$P_2 = c \cdot \log_2 \frac{n!}{(n-k)!}$$

The password space of the proposed scheme is: $P = P_1 \times P_2$. Choosing different parameters, for example increasing the values of k, n or c can increase security, but also decreases usability. We believe that remembering a key password and four images from different portfolios consisting of twenty images will not be a burden for users' memory, but it can increase the resistance to dictionary attacks by increasing password space in practice. Text passwords used in practice are generally far from randomly and independently selected. Most of the user passwords consist of only lowercase or digits which significantly decreases the entropy. For example, a randomly generated 8-character password consisting of digits (0–9), lowercase (a–z), and uppercase (A–Z) has $8 \cdot \log_2 62 = 47.6$ bits of entropy if all characters were selected randomly and independently. However, in practice they have far less bits than this [19]. Considering the realistic scenario, the added security from image selection parts of the proposed scheme becomes more significant. The integrated scheme significantly decreases the possibility of successful dictionary attacks.

Resistance to Attacks. As stated above, the proposed authentication scheme decreases the chance of attackers to obtain passwords via brute-force and dictionary attacks. The scheme has an integrated step of creating complex passwords based on text and images, which increases the numbers of possible passwords generated by the system, the password space.

While selecting the images and entering the associated characters, the input is given through keyboard rather than clicking on the images to prevent other people to observe the password over the user's shoulder. Allowing users to use mouse to enter the input maybe would make the system more adaptable but also more susceptible to shoulder surfing attacks. It supports client-server environment and its main advantage is the resistance to brute force and shoulder surfing attacks. However, the handicap of the scheme is that people who look over the user's shoulder can find out the previous character of the key password when they see the image portfolio. They of course, will not know the preferred image as users do not click on the images but this is still a risk for part of the password. This might be prevented by not placing images of objects, foods or famous people whose names' initials is same in a portfolio, but we prefer to evaluate its efficiency on memorizing images.

Usability Analysis. The idea of associating the images with the letters in the key passwords to increase the memorability of the final complex passwords come from the phenomenon called *Tip of the Tongue (TOT)*. The phenomenon refers to failing to retrieve a word from memory or partial recall but feeling that the retrieval is imminent [2, 9]. It reveals that lexical access occurs in several stages. People who experience this phenomenon can often recall some features of the target word mostly *the first letter*, or its syllabic stress and words similar in sound or meaning [3, 15]. The first letters of words are also important for coding words. For this purpose, phonetic alphabets are produced including code words which are assigned to each letter [7]. Users can code the words by assigning them to the letters in their key password to recall later. Associating the typed letters with images will help users to recall both the images and key characters.

Furthermore, to increase the memorability, the images in each portfolio are chosen from different categories including famous people, objects, sport activities, known art figures, animals, foods and places to be used in the authentication scheme similar to the Story scheme [8]. This allows users to have many options in which they can select the most appropriate one to themselves as well as the most probable one remember.

To evaluate the effectiveness of the scheme an empirical study was conducted with users. The next section presents the details of this study.

4 Methodology

An empirical study was conducted with the students at the University of Sussex in order to evaluate the security and usability of the proposed hybrid authentication scheme. In addition to the security and usability aspects, the study is

also used to evaluate the user satisfaction of the proposed scheme. To perform this study, an ethical approval was sought and obtained from the University of Sussex.

4.1 The Design and Apparatus

A web application was developed to test the security, usability and user satisfaction of the designed authentication scheme. The application also works on mobile phones enabling users to create strong passwords. The apparatus used in this study included a password register/login page of the designed authentication scheme; a questionnaire for the participants; and consent forms to read and accept for the participants.

First, the participants were asked to create an account using the scheme and login afterwards. The participants were shown a register / login page to enter their username and create a password. Once the participants had registered the application, they were given a questionnaire to fill out. The questionnaire included 6 questions related to users' experiences and satisfaction with the scheme. The average time to complete the study including registration and filling the questionnaire was approximately 10-15 minutes.

4.2 The Procedure

At the beginning of the empirical study, the participants were assigned a unique ID number. The participants were given information about the study and asked to read and accept the consent form. Once they had accepted the consent form, they were able to register the application. For those participants who were interested in getting more information about the study researcher's contact information were provided in the consent form. After the participants registered the application successfully, they were asked to fill the questionnaire. Participants were asked to login to the websites after a week and a month to find out whether they recall their passwords.

4.3 The Measurements

There are several measurements involved in the empirical study: the password strength, cracking time, creation and login time, memorability and user satisfaction. To measure the security of the new authentication scheme, created passwords were analysed using the "Password Meter" [13] and "How Secure is my Password?" [6] tools. While the "Password Meter" measured the strength of the passwords created with the scheme, "How Secure is my Password?" measured the password cracking times.

The other elements measured in this empirical study were the password creation and login times. The researcher measured these while participants were testing the authentication scheme. To measure the memorability, participants were contacted approximately after a week and a month, and asked to login the

system again to understand whether they remember or not their passwords. User satisfaction were measured based on questionnaire responses of the participants to evaluate the authentication scheme.

52 students studying in the University of Sussex were recruited to participate in this empirical study. There were 29 females and 23 male participants. Undergraduate students as well as postgraduate students participated in the study: 33 of the participants were undergraduate students, 19 of them were postgraduate students. Usability and security evaluation of the scheme based on the analysis of the collected data is presented in the following sections.

5 Results

Here we give the results and an analysis of the empirical study.

5.1 The Password Analysis

Password Strength. To evaluate the strength of the passwords created with the proposed authentication scheme, an empirical study was conducted with 52 participants. All the passwords created with the scheme were between 12 to 16 characters in length. Since eight characters come from the selected images provided by the scheme inherently, the length of user-chosen key passwords were 6 characters long on average. The "Password Meter" is used as a tool to measure the password strength. All participants created passwords with this scheme, and all of them were strong passwords according to the measurement results. The passwords created by the participants were scored out of 100 and the least score was 81, whereas the mean password strength was $M = 96.50(SD = 5.96)$. However, this tool alone is not sufficient to determine the resistance of a password to cracking. The user-generated passwords should be strong enough to password guessing attacks. The next section discusses the password cracking times of the passwords created with the proposed scheme by the participants.

Password Creation and Login Time. The password creation time and login time of the participants were measured by the researcher during the experiment. Table 1 summarizes the time it takes to create a password and to login in seconds. It took about one or two minutes on average to create a password or to login for participants.

Memorability. Passwords created with the proposed authentication scheme were remembered correctly most of the time. Although there was a slight decrease from a weeks duration to a month, still 75% of 52 participants remembered their passwords correctly, and successfully logged in to the system. Table 2 shows the login success rates after a week and a month period.

	Password Creation Time	Login Time
Proposed Authentication Scheme	$M = 94.08$ ($SD = 19.93$)	$M = 57.40$ ($SD = 15.73$)

Table 1. Password creation and login times in the empirical study.

	Login Success Rates (after a week)	Login Success Rates (after a month)
Proposed Authentication Scheme	90.38%(47/52)	75%(39/52)

Table 2. Login success rates in the empirical study.

5.2 The Results Based on the Survey Responses

User Satisfaction. Participants were asked about their experiences on the use of the novel authentication scheme to create an account. 92% of the participants liked the method of password creation with the scheme. 94% of them considered that it was fun to use, and similarly, 90% of the participants considered that the scheme was easy to use (see Figure 4).

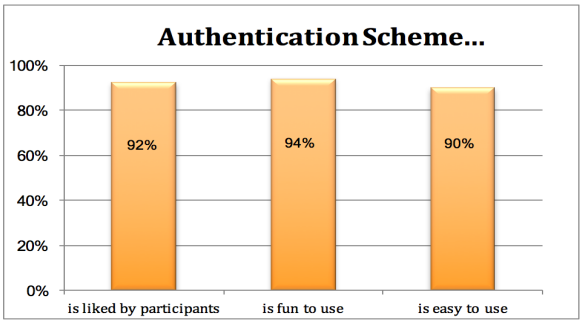


Fig. 4. Participants' opinion with regard to the use of the proposed scheme.

When it comes to the beliefs of participants in the method used by the proposed authentication scheme, results showed that most participants agreed that this method created stronger passwords than other commonly used methods (89%). However, agreement was less on creating more memorable passwords with

this method, though still more than half of the participants (58%) agreed that this method would create more memorable passwords. Figure 5 illustrates the participants' perception of the proposed schemes ability to allow users to create strong and memorable passwords. However, results of the experiments showed that the actual memorability rates were higher than participants expected.

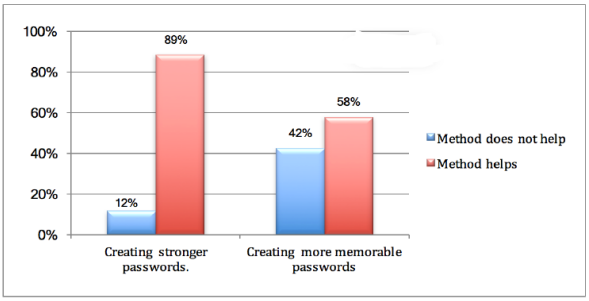


Fig. 5. Users perception of the proposed scheme's ability to produce strong and memorable passwords.

In addition to the users' thoughts of the efficiency of the new authentication scheme on creating strong and memorable passwords, they were also asked whether they will prefer to use the scheme or not. Only 5 out of 52 participants (9.6%) reported that they would not prefer to use the scheme neither for important passwords nor for others. On the other hand, 30 participants (32.7%) reported they would use the novel scheme for important passwords and 17 participants (57.7%) would use it for all passwords. The empirical study gave results that show the proposed authentication scheme provides usability and security, as well as high user satisfaction rates.

6 Discussion

Traditional text passwords alone are vulnerable to brute-force and dictionary attacks as users choose weak and predictable passwords in favour of memorability. On the other hand, graphical passwords alone are subject to shoulder surfing attacks. They also introduce usability issues by making password creation process longer for users. For these reasons, a hybrid authentication scheme integrating text and recognition-based graphical passwords is proposed in this paper. The design of the proposed scheme differs from other combined schemes since it offers an integrated registration phase rather than two or three different steps. It largely preserves the sign-in and log-in experiences of users who are accustomed to use text passwords. The proposed scheme does not suggest a discrete graphical password creation step, instead it uses the images as cues

to help users to create complex text passwords and memorize them easily. This also provides a usable authentication method by decreasing the steps of password verification. The proposed hybrid authentication method is implemented and an empirical study is conducted to evaluate its effectiveness on producing strong and memorable passwords.

Users authenticate themselves in a similar way as they do with conventional text-passwords, without increasing the registration time unreasonably. The small difference with the registration and login time can be tolerated whereas the additional security is added to the scheme over the usual text password authentication. In the empirical study, the participants used the authentication scheme to login only twice in a month. When this scheme is used for real systems, the login times are likely to decrease as the frequency of logging into the system will be higher. As time goes by, users will also be able to memorize their passwords and will not need to resort to images to enter the characters.

The resulting scheme is easy to use, and it helps users to create memorable as well as strong passwords which are resistant to dictionary attacks. Since the images in the registration phase are randomly placed in the portfolio every time, they include different characters for different users, and they are chosen by entering the characters under them through keyboard but not clicking on them provide a resistance to shoulder surfing attacks. It also provides a large password space by combining the text and images to create passwords. This reduces the possibility of cracking the passwords for third parties. The results of the study showed that password cracking times are significant so as to eliminate brute-force and dictionary attacks.

With regards to improving the proposed hybrid password authentication, an immediate endeavour that can be carried out is to investigate whether the relation between the typed character with the first letters of the names of objects, famous people, activities etc. in images affects the security. These relations have been inspired by the Tip of the Tongue phenomenon in the hope of increasing the memorability of passwords. In the conducted user study, the majority of the participants indeed remembered correctly their passwords but yet it is difficult to say if this is caused by the association between the key passwords characters and image portfolios. While expecting to increase usability, it might reduce the security by increasing the chance of shoulder surfing attacks. This is the dilemma of proposed scheme that need to be clarified so further investigations will be useful to find out the impact of associating typed characters with images on password security and memorability. This is an interesting research question as the challenge of balancing security and usability remains. It is also worthwhile making slight modifications on the scheme in order to increase usability. For example, the characters placed under the images can be changed each time even for the same user which means creating a one-time password each time. The security and usability evaluation of such scheme might yield interesting results.

References

1. Adams, A., Sasse, M.A.: Users are not the enemy. Communications of the ACM **42**(12), 40–46 (1999). https://doi.org/10.1145/322796.322806
2. Brown, A.: A review of the tip-of-the-tongue experience. Psychological bulletin **109**(2), 204–223 (1991)
3. Brown, R., McNeill, D.: The tip of the tongue phenomenon. Journal of Verbal Learning and Verbal Behavior **5**(4), 325–337 (1966)
4. Burnett, M., (Ed.), D.K.: Perfect Passwords. Syngress Publishing, Inc. (2006)
5. Chen, Y.L., Ku, W.C., Yeh, Y.C., Liao, D.M.: A simple text-based shoulder surfing resistant graphical password scheme. In: IEEE 2nd International Symposium on Next-Generation Electronics. pp. 161–164. IEEE (Feb 2013). https://doi.org/10.1109/ISNE.2013.6512317
6. Collider, S.: How secure is my password? `https://howsecureismypassword.net` (2016), [Online; Accessed 14 January 2017]
7. Crystal, D.: Dictionary of linguistics and phonetics, vol. 30. John Wiley & Sons (2011)
8. Davis, D., Monrose, F., Reiter, M.: On user choice in graphical password schemes. In: Proceedings of The 13th USENIX Security Symposium. pp. 151–164. USENIX Association, San Diego, CA, USA (2004)
9. Encyclopedia.com: Tip-of-the-tongue phenomenon - dictionary definition of tip-of-the-tongue phenomenon. `http://www.encyclopedia.com/psychology/encyclopedias-almanacstranscripts-and-maps/tip-tongue-phenomenon`, [Online; Accessed 9 Nov. 2016]
10. Haque, M., Imam, B.: A new graphical password: Combination of recall & recognition based approach. International Journal of Computer, Electrical, Automation, Control and Information Engineering **8**(2), 320–324 (2014)
11. Haque, M., Imam, B., Ahmad, N.: 2-round hybrid password scheme. International Journal of Computer Engineering and Technology (IJCET **3**(2), 579–587 (2012)
12. Mokal, P., Devikar, R.: A survey on shoulder surfing resistant text based graphical password schemes. International Journal of Science and Research (IJSR) **3**(4), 747–750 (2014)
13. Passwordmeter.com. (n.d.): Password strength checker. `http://www.passwordmeter.com` (2017), [Online; Accessed 5 Jan. 2017]
14. Rao, K., Yalamanchili, A.: Novel shoulder-surfing resistant authentication schemes using text-graphical passwords. International Journal of Information and Network Security **1**(3), 163–170 (2012)
15. Schwartz, B., Metcalfe, J.: Tip-of-the-tongue (TOT) states: Retrieval, behaviour, and experience. Memory & Cognition, **39**(5), 737–749 (2011)
16. Shepard, R.: Recognition memory for words, sentences and pictures. Journal of Verbal Learning and Verbal Behaviour **6**, 156–163. (1967)
17. Sreelatha, M., Shashi, M., Anirudh, M., Ahamer, M., Manoj Kumar, V.: Authentication schemes for session passwords using color and images. International Journal of Network Security & Its Applications **3**(3), 111–119 (2011)
18. Van Oorschot, P., Thorpe, J.: Exploiting predictability in click-based graphical passwords. Journal of Computer Security **19**(4), 669–702 (2011)
19. Van Oorschot, P.C., Wan, T.: Twostep: An authentication method combining text and graphical passwords. International Conference on E-Technologies pp. 233–239 (2009)

20. Vorster, J., van Heerden, R.: A study of perceptions of graphical passwords. https://www.researchgate.net/publication/283712970_A_Study_of_Perceptions_of_Graphical_Passwords (2015), [Online; Accessed 2 Jun. 2016]
21. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password memorability and security: Empirical results. IEEE Privacy & Security **2**(5), 25–31 (2004)
22. Zhang, Y., Monrose, F., Reiter, M.K.: The security of modern password expiration: An algorithmic framework and empirical analysis. In: Proceedings of the 17th ACM conference on Computer and communications security. pp. 176–186 (2010)
23. Zhao, H., Li, X.: S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In: Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference. vol. 2, pp. 467–472 (May 2007). https://doi.org/10.1109/AINAW.2007.317