DUJASE Vol. 7 (1) 29-37, 2022 (January) *https://doi.org/10.3329/dujase.v7i1.62884*

A Practical Scheme to Improve Memorability of System-assigned Random Password

Fairuz Nawer Meem, Rahat Al Noman, Pritom Saha, Muhammad Shakil Pervez, Ismat Rahman, Moinul Zaber and S. T. Ahmed Rumee*

Department of Computer Science and Engineering
University of Dhaka, Dhaka-1000, Bangladesh

**E-mail: rumee@cse.du.ac.bd*

Received on 16 February 2021, Accepted for publication on 25 November 2021

ABSTRACT

Most users follow common strategies and patterns while choosing passwords, which makes them easier to remember but often very weak in terms of security. System-assigned random passwords can be an answer to this problem. However, these random passwords are difficult to remember and hardly used by the users through their strong security guarantee. Recently researchers have been trying on devising techniques to remember random passwords. However, state-of-the-art methods have noticeable limitations such as - no upper case or special characters were considered, which is not practical for any good password. This paper proposes a novel scheme to aid users in remembering random passwords that do not suffer from these limitations. Users can select both graphical and text-based hints and associate them with system-assigned random passwords. Detailed user surveys were performed and the results showed that the proposed method can help users to remember random passwords with high accuracy. Using the proposed method, participants could recollect random passwords with an accuracy of 90.41% (average), which becomes 95% if case sensitivity is ignored.

Keywords: Random Password, Memorability, Graphical Cue, Passphrases

1. Introduction

For authentication to any system or service, passwords are the go-to method. It is easy to use and widely adopted by almost all users. However, the ease of use comes with some genuine problems which often makes passwords the weakest link in system security.

People often choose passwords that are easy to remember (involving common patterns, name of relatives, national id no, birth year, etc.) and also use the same password in multiple accounts [1], [2]. The task of ensuring great usability and strength in case of choosing passwords is not straight forward. Numerous studies found that this behavior is common even after people know about the pitfalls of badly chosen passwords [3] – [5].

Researchers have been investigating the usability of random passwords for some time as a solution to the above-mentioned problems. Random passwords are system generated and free from any kind of user biases, so it will be extremely difficult for attackers to guess or crack them. At the same time, they are also horrible in terms of usability. Often these passwords are provided to users as the introductory token and advised to change after first use. So, researchers are trying to find ways that will give users cues/hints so that they can use such passwords instead of throwing them out. The goal is to train users with hints that can make them remember random passwords easily.

However, existing work e.g. [6] – [8] etc. on making random passwords memorable to users have significant limitations - no special character, no uppercase letter, very limited length, etc. Random passwords are itself difficult to remember and accommodating these special cases make them further challenging for users to actually recollect them after a while. So, random passwords still need a lot of improvement before being accepted as usable as traditional passwords.

Here, the primary goal of this work is to address some of these gaps and make the case for further research to make the system-assigned random password more usable. To realize this goal, we propose a novel scheme of using graphical cues that will aid users to remember system-generated random passwords. Our work has the following major contributions, which are mostly lacking in the existing methods:

- We used random passwords of length 8, which is standard for many systems/services and an improvement over the state-of-the-art method that considers maximum 6 character long passwords.
- Use of both uppercase and lowercase letters in password is considered.
- The presence of special characters in passwords (missing in the state-of-the-art methods) is also accommodated.

The proposed system was extensively validated through a series of user surveys. The findings of these studies prove that our system can help users to create graphical hints and use them to remember random passwords with high accuracy.

The rest of the paper is organized as follows. Section 2 introduces a number of key terminologies related to our research. Then few closely relevant works regarding the memorability of random passwords are discussed in section 3. The proposed method and the supporting user surveys are described in section 4. Then, section 5 presents the findings of the user survey. Finally, section 6 concludes the papers with an overall summary of this research and some possible directions for future work.

2. Key Terms and Definitions

2.1. Social Engineering:

In the context of information security, the psychological manipulation of people into performing actions or divulging confidential information is known as social engineering. It has also been defined as any act that influences a person to take an action that may or may not be in their best interests [9].

2.2. Shoulder Surfing:

Shoulder surfing is a type of social engineering techniques used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder.

2.3. Dictionary Attacks:

In Cryptanalysis and computer security, a dictionary attack is a form of brute force attack technique for defeating a cipher or authentication mechanism. Here the effort is made to determine the decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

Dictionary attacks often succeed because many people have a tendency to choose short passwords that are ordinary words or common passwords, or simple variants obtained, for example, by appending a digit or punctuation character.

2.4. Chunking:

In cognitive psychology, chunking is a process by which individual pieces of an information are broken down and then grouped together. For example, when recalling a number such as 12101946, if numbers are grouped as 12, 10 and 1946, a mnemonic is created for this number as a day, month and year.

2.5. The Von Restorff Effect:

Also known as the "isolation effect", predicts that when multiple homogeneous stimuli are presented, the stimulus that differs from the rest is more likely to be remembered [10]. For example, if a person examines a shopping list with one item highlighted in bright green, he or she will be more likely to remember the highlighted item than any of the others.

2.6. Spatial Cueing:

Visual spatial attention is a form of visual attention that involves directing attention to a location in space. Spatial attention allows humans to selectively process visual information through prioritization of an area within the visual field. Research shows that when spatial attention is evoked, an observer is typically faster and more accurate at detecting a target that appears in an expected location compared to an unexpected location [11].

3. Related Work

Remembering passwords with graphical hints has got a significant level of attention from researchers recently. Here we limit our discussion to the work closely related to our proposed method.

Suo et al. [12] give a nice summary of existing work on using graphics or images as a password or password hints. It paved the way for further investigation in this regard and a lot of studies have been performed based on the finding of this seminal work.

At first, a graphical password technique by Leonardo et al. [13] was developed which deals with the shoulder surfing problem. Later [11], [14] represented the advantages of passphrases which are often more memorable over a long duration of time. It has been found by Brostoff et al. [15] that text-based passwords have three times more login failure rate than passphrases.

The first known work to aid users with remembering system-assigned random passwords is described in CuedR [16]. Here users are provided multiple cues. These cues can be categorized into three types: visual, verbal, and spatial. Users are allowed to choose any of the given options from any category which seems easier for them to recall. Although this method resulted in 100% memorability, it suffers from the following major limitations: No user-level interaction, no relation between the cues, and users are only considered to be within a certain age level.

Similarly, researchers in [17] – [20] propose schemes to use graphical hints to remember passwords. However, none of them could improve the memorability issue of system-assigned random passwords. Moreover, memory research shows that recalling any particular word or picture or password becomes harder without having any memory link [21], [22].

Later on, Al-Ameen et al. [23] offer both spatial cues (fixed position of images on the screen) and verbal cues (phrases/facts related to the images). For creating different study conditions, face images along with object images were used to find out which ones are easier to recall. This approach employs user interaction at the registration level where users have to write a short description about the images, making them easily memorable. Similarly [21], [24]–[26] stresses that recognition helps better than recall to remember any picture or word.

The most closely related work is done by Haque et al. [27]. It employs a three-dimensional spatial navigation scheme to find artifacts related to the characters of a system-assigned random password. Though it has a high success rate and solves many existing problems, it does not consider cases that are commonly seen in any good password, such as - both uppercase and lowercase letters, passwords having more than six characters, and special characters. The proposed method particularly aims at these cases to overcome the shortcomings of this breakthrough work.

4. Methodology

To investigate the memorability of random passwords, the proposed system is based on a web interface for recording user interaction (survey) and then analyzing it.

At first, a participant register for his account in the web interface, and a system-generated random password is generated for that user. Users go through a training phase where they choose hints for the selected password. Later on, participants try to log in and use the hints chosen during password creation if required.

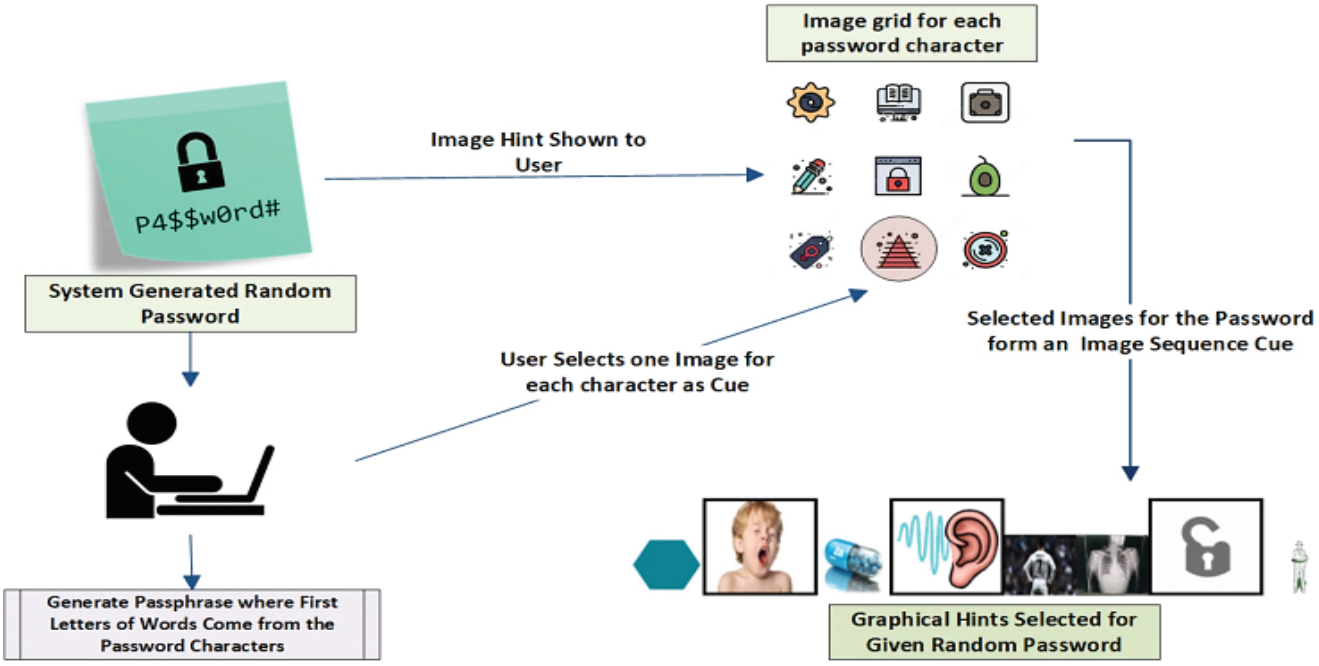

Fig. 1. User Activity in Training Phase

This section gives an overview of our methodology (using both graphical and textual cues) to help users remember this seemingly difficult random password and analyze user behavior (the ability to use cues for password recollection). A high-level overview of the workflow involved in user training during the password creation (registration) phase is shown in Figure 1. An important cornerstone of the proposed method is the way graphical cues are generated. An overview of this cue generation strategy is also given here.

4.1. User Survey Process

This User study is done in two phases. During the training (Phase 1), users are assigned random passwords when they create a new user in the web-based interface. In Phase 2 (one week after Phase 1), users try to re-login using credentials and hints created in phase 1.

1) Phase 1: Training(Registration) Phase: During the registration phase, each user is assigned a random password consisting of eight characters (alphanumeric letters, digits, and few special characters).

Next, users are directed to go through a series of web interfaces to select an image (hint) for each character. Images appear on a grid and when a particular picture is chosen, the user will be shown his/her selection in a spatial cue with other non-selected options blurred to provide the von Restorff or isolation effect for better memorability.

Similarly, digits in the password will be assigned relevant image cues. As an example, for number '1', we can show the picture of Shakib Al Hasan as many users can relate Shakib as the number one all-rounder. On the other hand, special characters will be handled based on their shape.

In addition to associating images with password characters, users will also optionally create a passphrase (a meaningful statement with the first letters of the words coming from the password characters). This will be used as an additional hint alongside the graphical cues. However, this passphrase will only be known to the user which he can later use to recollect the password. So, remembering it falls under the jurisdiction of users. Our system just inspires users to create this additional hint to aid password recollection.

In the training phase, image grids are shown with additional effects (partial blurring, animations) to help users distinguish between different types of characters. These additional effects are only shown at the password creation phase and are not accessible to attackers. Here, our hypothesis is users can recollect their random passwords using these additional effects, which are not available to any third party.

2) Phase 2: Testing(Login) Phase: During login phase, the user tries to log in to the system again using the password created in phase 1. If required, users will be provided a hint for each character of the password using an image grid,

which contains the chosen image for that character in phase 1 and 5 other randomly selected but relevant images.

To offset the attackers or any unauthorized access, no additional hint rather than the image options is given. In this phase, no additional cue on position, case (lower or upper), and type (regular or special) of a password character was given, the case was chosen, and whether that position belongs to an uppercase letter or special character.

Users can also take the help of a passphrase (if it was created during phase 1) to recall the sequence of password characters along with their correct positions. This is just an option the legitimate user has and no other person has access to it. The system does neither stores passphrase information nor shows it to users as a hint in any stage of the proposed method.

4.2. Graphical Cue Generation Details in Password Creation Phase (Phase 1)

Random passwords are difficult to guess for attackers and at the same time have little use rather than the initial password for any system. However, any methodology to use such random passwords and remember them must involve some form of cues that will help users to recollect them. In this work, we used graphical cues in the form of image grids.

The details of this cue generation are outlined below.

1) Handling Alphanumeric Characters: As discussed before, users are guided to select an image hint from a grid of relevant images for each character of the password. Grid size and content are carefully chosen to help users remember their choice and attackers cannot apply any brute force method to crack it.

Fig. 2. Images representing letter ‘b’

To add confusion, which is the essential quality of any strong password, all the options shown in a grid have the potential to be a representative for the password character in question. For example, the Figure 2 shows options generated by our system for letter ’b’. These options are purely random and will be chosen from a large pool of images all representing letter ’b’ for further invocations.

The user has to select any of the pictures from the given options and repeat for each character in the password. To help the user remember his selection the chosen picture will be shown again with other images blurred (Figure 3).

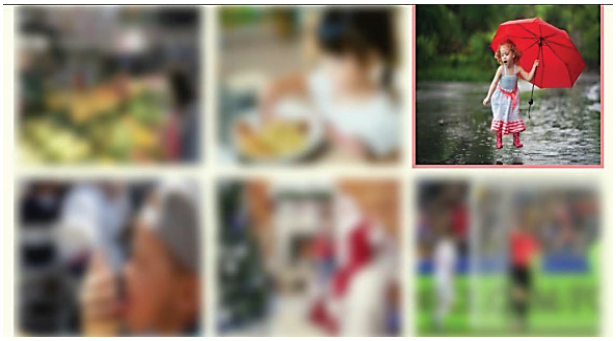

Fig. 3. Selected image for letter ‘b’

Like this, a corresponding image hint is selected for each character of the random password. Then the selected image hints are displayed together again (Figure 4) to consolidate users’ memory about this his/her password choice.

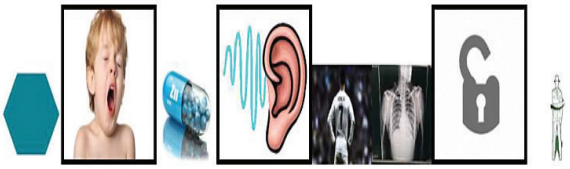

Fig. 4. User selected images for a random password

2) Distinguish Character Cases: One of the primary challenges was to distinguish between the uppercase and lowercase letters. To solve this, we use an additional layer of a hint by adding animation to the image grid related to an uppercase letter.

For uppercase characters, the selected image from the image grid is given a blink effect to animate it while the other images remain blurred. From our experiment, we found that this has a success rate in reminding users of the cases of the password characters.

3) Handling Special Characters: Special characters are also represented by eight relatable images in a grid. To aid users to remember that a certain position of the password is occupied by the special character, we add an additional hint as we did in the case of uppercase letters.

Here, after selecting an image from the grid we show a large thick border around the selected image while blurring the other options. No animation is added to distinguish it from uppercase letters.

4.3. Usage of Passphrases

Alongside the picture hints, users also have the option to create a passphrase (comprising of words starting with the letters in the system assigned password). To make this scenario or passphrase, the users have to think about the words multiple times, thereby expected to help them remember the password. The proposed system just facilitates

users to create this passphrase and it is not part of our system. It is kind of guiding users to create additional hints to remember the random password. Our system does not save the passphrase information and it is only available to the user himself/herself.

5. User Study Findings

This section discusses the user studies we conducted to validate the proposed method. At first, a pilot study is done on 8 users, and results were found to be promising. Later, more users were incorporated and the survey outcome further consolidated the findings of the pilot study. User responses are anonymized to ensure privacy and security.

In the following, we first describe the details of the survey design and later present the findings in terms of usability and memorability of the proposed method.

5.1. User Demographics

The initial pilot study involved 8 users (students of IT or relevant majors). Based on the findings, we modified our system and performed a second study involving 10 users. Here we surveyed 5 IT Major students and 5 from the non-IT background (2 from medical science and 3 having business major). We again adjust our methodology based on the findings.

Table 1: Demographic of survey participants

Profession	Number of Participant
University Students	8
Doctors	5
Military Personnel	4
Government Employees	4
Engineers	5
Bank Employees	4
Total	30

Finally, we surveyed 30 more participants involving people of different educational and social backgrounds. The demographic of participants are listed in Table 1.

5.2. Pilot Study

The pilot study involved eight participants. They were given randomly generated passwords and options to create hints from image grids. Based on that, the participants chose images corresponding to the characters in their passwords. The selected images will act as hints for a future attempt to accessing the system using that password. Here, we examined whether the proposed system involving graphical cues helps users to recollect a system-assigned random password. We also examined the scenario of how good is this method if the users do not include the optional passphrase creation phase during the registration (training) stage.

As shown in Table 2, user performance was measured in terms of time required for the registration phase. As part of the study, survey respondents are required to log in to their accounts after seven (7) days. It is tested to see if they can do that by recollecting their password from memory and using the hints they created earlier. The results are shown in (Table. 3).

From this result of the pilot study, it was visible that the sentence hint (passphrases) helps the users to recall the password. Those who did not create or take help from passphrases have higher login times than others.

Table 2: User training time(pilotstudy- phase 1)

User No.	Graphical Cue	Generation Time (minutes)
	Without passphrase	With passphrase
1	2.63	3.72
2	2.24	3.3
3	1.61	1.8
4	3.72	3.43
5	2.47	3.62
6	2.3	3.26
7	1.65	1.98
8	1.3	2.12

Table 3: Login success rate (pilot study- phase2)

User No.	Used Pass-phrase?	Successful Login	Login Time (mins)
1	Yes	Yes	2.4
2	Yes	Yes	3.7
3	Yes	Yes	2.8
4	Yes	No	0.0
5	Yes	Yes	3.2
6	Yes	Yes	1.67
7	No	Yes	4.1
8	Yes	Yes	0.57

Table 3 shows that even without passphrases, only one out of eight users failed to log in. This finding suggests that the image grid options and relevant additional hints (for case sensitivity handling and special characters) are also successful in remembering the random passwords. We also gathered feedback from the user who could not log in without passphrase help and found that he did not create a meaningful passphrase, so failed to use it later on.

The feedback obtained in this preliminary study helped us to update the graphical cue generation strategy greatly to add more confusion for the potential attackers and make the proposed system more resilient. As part of the updates, we introduced additional animations during the training phase to help users distinguish lowercase and uppercase characters. Similar measures were also taken for special characters in the password.

5.3. Second User Survey and System Modifications

Here, we repeat the experiment done on the pilot study with more users and most importantly with the modified system based on the feedback received in the pilot study. To get a perspective on the attackers' side, all usernames created in this study were provided to every user and they were asked to guess the password of other users.

Table 4: Second survey results (login success rate during training)

User No.	Original Password	Typed Password	Correctness (In Terms of Case Sensitivity)	
			Yes	No
1	8Ti8jb8s	8Ti8jb8s	8/8 (100%)	8/8 (100%)
2	gExz2Qqx	gExz2dqx	7/8 (87.5%)	7/8 (87.5%)
3	nD882jGS	nD882jGS	8/8 (100%)	8/8 (100%)
4	0Bo0NOmA	0Bo0NOma	7/8(87.5%)	8/8 (100%)
5	07vDwh20	07vDwh20	8/8 (100%)	8/8 (100%)
6	z246UIhz	z246UIhz	8/8 (100%)	8/8 (100%)
7	p4WT2QEo	p4WT2QEo	8/8 (100%)	8/8 (100%)
8	cyh54eIE	cyh54eIE	8/8 (100%)	8/8 (100%)
9	4oaRGq9f	4oaRGq9f	8/8 (100%)	8/8 (100%)
10	EyBZyr84	eyb0yr84	5/8 (62.5%)	7/8 (87.5%)
			Avg: 93.75%	**Avg: 97.5%**

At first, images showed in the selection section were being displayed as a hint and the guessing of that particular letter or number becomes easier. For example, if any user sees a baby yawning picture as a hint s/he will find it difficult to guess whether it is for 'baby' or 'yawn'. But if multiple pictures are resembling 'y' like yoga, yeast, yolk then the user becomes sure that the picture indicates the letter 'y'.

So the approach was changed a little bit later and the users were shown only their selected pictures accompanied with new random images which are relevant (some of them may have appeared before in the image grid during training and some are new) as hints. This time no user could guess any other user's password despite being given the hints.

Table 4 shows the login success rate during the training phase. Here we updated our data set and used the same pictures for multiple characters to create more confusion for the attackers. The second survey involved 10 people and the success rate was measured at 93.75% considering case sensitivity and 97.5% ignoring the cases.

A high success rate is expected as this login attempt was made immediately after the training. This was done to validate whether the training methodology worked for the users.

Table 5: Second survey results (login success rate during testing)

User No.	Correctness (Case Sensitive)	Correctness (Not Case Sensitive)
1	5/8 (62.5%)	7/8 (87.5%)
2	7/8 (87.5%)	7/8 (87.5%)
3	3/8 (37.5%)	4/8 (50%)
4	7/8 (87.5%)	8/8 (100%)
5	6/8 (75%)	8/8 (100%)
6	5/8 (62.5%)	8/8 (100%)
7	8/8 (100%)	8/8 (100%)
8	8/8 (100%)	8/8 (100%)
9	8/8 (100%)	8/8 (100%)
	Avg: 79.16%	**Avg: 91.66%**

The findings are promising as we can assume this was only possible because of graphical hints. Without those cues, it is excessively difficult to remember random passwords even during the training phase.

To measure the memorability of our proposed approach, we repeat the process with the same users after one week. This time one of the participants could not join and we had nine of our previous respondents. The result of this survey (testing phase measuring user memorability) is shown in Table 5.

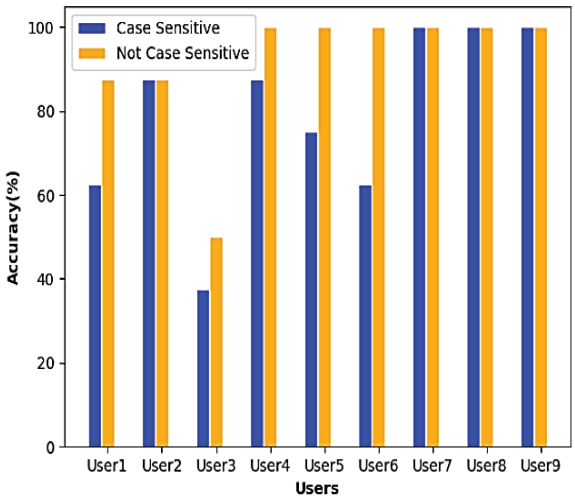

Fig. 5. Login Success Rate Comparison Regarding Character Cases

Figure 5 further highlight these findings showing the difference in user's memorability based on whether we ignore the cases of passwords characters or not.

To remove the confusion between lowercase and uppercase letters, we add an additional animation (blinking the selected image in the grid) for uppercase letters in the training session to help the users distinguish between the uppercase and lowercase letters while recalling the password. This had a huge effect on memorability and the login success rate increased by a noticeable rate (Figure 6).

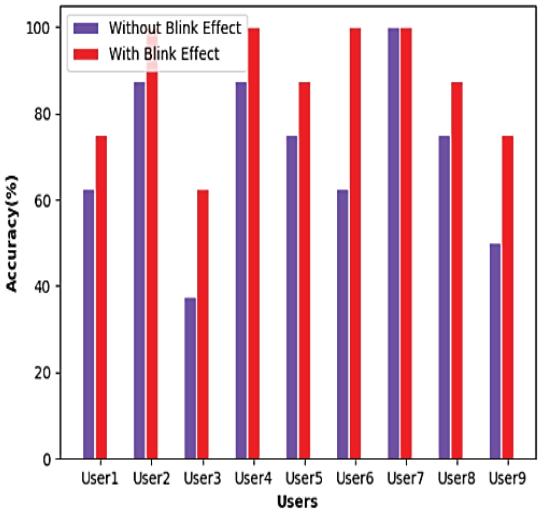

Fig. 6. Login Success Rate Increased after Blink Effect Integration for Uppercase Letters

5.4. Third User Survey

Based on the 2nd user survey findings, we incorporated all the suggestions and policy updates in the proposed method and performed a detailed study involving 30 users. The demographic of participants are already discussed previously and shown in Table 6.

Table 6: User performances in final survey on proposed system (login success rate)

User No.	Original Password	Typed Password	Correctness (In Terms of Case Sensitivity)	
			Yes	No
1	hB2uF9W6	hB2uF9W6	8/8 (100%)	8/8 (100%)
2	gExz2eQX	gExz2dqx	5/8 (62.5%)	6/8(75%)
3	nD882jpa	nD882jGS	6/8(75%)	6/8(75%)
4	v7YPSmDR	v7YPSmDR	8/8 (100%)	8/8 (100%)
5	89gHgQqy	89gHgQqy	8/8 (100%)	8/8 (100%)
6	xnZgRd5M	xnZgRd5M	7/8 (87.5%)	7/8(87.5%)
7	55vreT88	55vreT88	8/8 (100%)	8/8 (100%)
8	67Bhr7ZC	67Bhr7ZC	8/8 (100%)	8/8 (100%)
9	2shDd6Xb	2shDd6Xb	8/8 (100%)	8/8 (100%)
10	Ydmt3WuP	Ydmt3WuP	7/8 (87.5%)	7/8(87.5%)
11	TXTvJy4m	TxTvJa4p	5/8(62.5%)	7/8(87.5%)
12	hzn4ED8H	hzn4ED8H	8/8 (100%)	8/8 (100%)
13	aWN49z8t	aWN49z8t	8/8 (100%)	8/8 (100%)
14	FYwtJt7S	FYwtJt7S	8/8 (100%)	8/8 (100%)
15	3FNC2wee	3FNC2wee	8/8 (100%)	8/8 (100%)
16	hd5RXkk9	hd5RXkk9	8/8 (100%)	8/8 (100%)
17	8vD3tTkh	8vD3tTyh	7/8(87.5%)	7/8(87.5%)
18	c5B8UvwY	c5B8UvwY	8/8 (100%)	8/8 (100%)
19	2LsDyXh9	2LsntXh9	6/8(75%)	6/8(75%)
20	FkQvHa8G	FkQvty8G	6/8(75%)	6/8(75%)
21	kqz6J7Tq	kqz6J7Tq	8/8 (100%)	8/8 (100%)
22	W8m7RLQB	W8m7RLQB	8/8 (100%)	8/8 (100%)
23	2sy979BJ	2sy979BJ	8/8 (100%)	8/8 (100%)
24	eaNA7n4B	eaNL7n4B	7/8(87.5%)	7/8(87.5%)
25	bDHQj2Ek	bDHqj2Ek	7/8(87.5%)	8/8 (100%)
26	9eJjKFkQ	9eJjuFkQ	7/8(87.5%)	7/8(87.5%)
27	3y8Krkdb	3y8KECdb	6/8(75%)	6/8(75%)
28	2LcVjLDg	2lcvjLdg	5/8(62.5%)	8/8 (100%)
29	PM8qqXmh	PM8qqXmh	8/8 (100%)	8/8 (100%)
30	5cFgcJ9Q	5cFgcJ9Q	8/8 (100%)	8/8 (100%)
			Avg: 90.41%	**Avg: 95%**

The results show that the proposed method helps users remember graphical passwords (combination of alphanumeric and special characters) with high accuracy (more than 90%), where the state-of-the-art method can only achieve similar outcomes considering only alphanumeric characters and ignoring character cases or special characters [27].

Here, we observe an average success rate of 90.41% considering case sensitivity. It becomes 95% if case sensitivity is ignored.

5.5. Analysis of Users' Feedback and Discussion

Apart from experimenting with the proposed method, we collected and analyzed information about the password choic e of the survey participants. According to the responses, 57.1% of users never use system assigned random passwords and among them, 86.3% of users choose to use system-assigned random passwords if they are made memorable. 50% of those who use system-assigned passwords agreed with the fact of facing difficulty remembering the password.

The users also answered some questions regarding our approach. 85.7% users found out the sentence hint helpful to recall the password and 64.3% users said the process was not too much longer to get irritated or bored. We asked the users about the hardest part of recalling the password. According to their response, 14.3% users faced difficulty in retrieving digits from the chosen picture, 21.4% users found difficulty in retrieving the correct letter from the selected pictures while 64.3% users were confused between uppercase and lowercase letters.

Among all participants, 85.7% of users found this approach to help recall system-assigned random passwords. We asked for some suggestions from the participants and the most common suggestion was to present a better approach for differentiating between the uppercase and lowercase letters.

6. Conclusion

This work investigated how to improve the memorability of random passwords- which are difficult to guess/remember but have strong security. In this regard, we proposed to use a traditional image grid as a password hint and also took the help of meaningful passphrases. Their combined effect was proved to be successful and the experiment shows that users can remember randomly generated passwords using the hints proposed in this work.

The assumptions behind the primary contributions of this paper are fairly common in the passwords we generally use but very much challenging in terms of system-assigned random passwords. To the best of our knowledge, no existing work has dealt with the factors (mentioned in the list of contributions above) in the case of remembering random passwords.

We assume random passwords are not that popular because of their difficult-to-remember structure and as a result not been investigated fully by the researchers yet. it is a long way to go before making random passwords fully usable. This work is also aimed at finding solutions to some of the key limitations in remembering system-assigned random passwords but does not guarantee to be a complete solution. Such a solution will require a significant contribution from the research community and will take time. We believe, our work is a significant step towards that goal and will help future researchers to develop a fully robust method that will help users to easily get used to random passwords of all kinds (considering passwords having an arbitrary length and full set of characters available in regular passwords).

Following are some of the future work:

- Consider more types of special characters.
- Punctuation characters should be considered also.
- Consider passwords of length greater than 8.

References

1. J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *IEEE Security & privacy*, vol. 2, no. 5, pp. 25–31, 2004
2. B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Communications of the ACM*, vol. 47, no. 4, pp. 75–78, 2004.
3. S. Furnell and R. Esmael, "Evaluating the effect of guidance and feedback upon password compliance," *Computer Fraud & Security*, vol. 2017, no. 1, pp. 5–10, 2017.
4. N. Kumar, "Password in practice: An usability survey," *Journal of Global Research in Computer Science*, vol. 2, no. 5, pp. 107– 112, 2011.
5. S. Furnell, "Assessing website password practices–over a decade of progress?" *Computer Fraud & Security*, vol. 2018, no. 7, pp. 6–13, 2018.
6. A. Constantinides, M. Belk, C. Fidas, and G. Samaras, "On cultural-centered graphical passwords: Leveraging on users' cultural experiences for improving password memorability," *in Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization*, 2018, pp. 245–249.
7. M. N. Al-Ameen, S. T. Marne, K. Fatema, M. Wright, and S. Scielzo, "On improving the memorability of system-assigned recognition-based passwords," *Behaviour & Information Technology*, pp. 1–17, 2020.
8. M. Mohamed, J. Chakraborty, and S. Pillutla, "Effects of culture on graphical password image selection and design," *Journal of Systems and Information Technology*, 2020.
9. L. A. Harper, The English Navigation Laws: a seventeenth century experiment in social engineering. *Columbia University Press, New York*, 1939.
10. H. Von Restorff, "The effects of field formation in the trace field," *Psychol Res*, vol. 18, no. 1, pp. 299–342, 1933.
11. T. Valentine, "An evaluation of the passface personal authentication system, goldsmith college univ," of London, *Tech. Report, Tech. Rep*., 1999.
12. X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *21st Annual Computer Security Applications Conference (ACSAC'05). IEEE*, 2005, pp. 10–pp.
13. S. Leonardo, "Graphical pass-words, the rutgers scholar an electronic bulletin of undergraduate research," http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg. htm, 2008.
14. T. Valentine, "Memory for passfaces after a long delay," *Report to ID Arts*, 1999.
15. S. Brostoff and M. A. Sasse, "Are passfaces more usable than passwords? a field trial investigation," in *People and computers XIV—usability or else! Springer*, 2000, pp. 405–424.
16. M. N. Al-Ameen, M. Wright, and S. Scielzo, "Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 2315–2324.
17. K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2009, pp. 889–898.
18. A. Forget, S. Chiasson, P. C. Van Oorschot, and R. Biddle, "Improving text passwords through persuasion," in *Proceedings of the 4th symposium on Usable privacy and security*. ACM, 2008, pp. 1–12.
19. R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "Correct horse battery staple: Exploring the usability of system-assigned passphrases," in *Proceedings of the eighth symposium on usable privacy and security*. ACM, 2012, p. 7.

20. N. Wright, A. S. Patrick, and R. Biddle, "Do you see your password?: applying recognition to textual passwords," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 8.

21. J. R. Anderson and G. H. Bower, "Recognition and retrieval processes in free recall." *Psychological review*, vol. 79, no. 2, p. 97, 1972.

22. E. Tulving, "Synergistic ecphory in recall and recognition." *Canadian Journal of Psychology/Revue canadienne de psychologie*, vol. 36, no. 2, p. 130, 1982.

23. M. N. Al-Ameen, K. Fatema, M. Wright, and S. Scielzo, "The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords," in *Eleventh Symposium on Usable Privacy and Security* ({SOUPS} 2015), 2015, pp. 185–196.

24. E. Tulving and M. J. Watkins, "Continuity between recall and recognition," *The American Journal of Psychology*, pp. 739–748, 1973.

25. W. A. Wickelgren and D. A. Norman, "Strength models and serial position in short-term recognition memory," *Journal of Mathematical Psychology*, vol. 3, no. 2, pp. 316–347, 1966.

26. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes." in *USENIX Security Symposium*, vol. 13, no. 2004, 2004, pp. 11–11.

27. S. T. Haque, M. N. Al-Ameen, M. Wright, and S. Scielzo, "Learning system-assigned passwords (up to 56 bits) in a single registration session with the methods of cognitive psychology," *Proc. USEC. The Internet Society*, 2017.