A Shoulder-Surfing Resistant Scheme Embedded in Traditional Passwords

Jianwei Lai
Illinois State University
jlai12@ilstu.edu

Ernest Arko
Illinois State University
earko@ilstu.edu

Abstract

Typing passwords is vulnerable to shoulder-surfing attacks. We proposed a shoulder-surfing resistant scheme embedded in traditional textual passwords in this study. With the proposed scheme, when the password field is on focus, a pattern appears in it as a hint to tell the user how to enter a password. Following the hint, the user needs to skip some characters while typing the password. The characters to be skipped are randomly selected so that an observer will not be able to see the whole password even if the authentication procedure was recorded. We evaluated the proposed scheme in a usability study. Compared to traditional passwords, our scheme achieved a similar level of accuracy while only required marginal additional time to authenticate users. Participants also expressed significantly higher acceptance of the new technique for security-sensitive applications and gave it significantly higher ratings in perceived security, shoulders-surfing resistance, camera-recording resistance, and guess-attack resistance.

1. Introduction

Passwords are the most prevalent user authentication method on current digital devices [1, 2]. Given the important role of passwords, it is critical to keep them safe. Traditional passwords are alphanumeric [3]. They require users to enter them with keyboards. However, typing on keyboards is vulnerable to observation attacks, such as shoulder-surfing, which means stealing users' information, such as passwords, PINs, and other sensitive information, by looking over someone's shoulder [1, 2]. Shoulder-surfing is quite common in real life [4], but quite difficult to defeat [1, 5]. The popularity of recording devices, such as mobile phones, surveillance cameras, etc., make shoulder-surfing even easier. It is important to make passwords shoulder-surfing resistant, especially for security-sensitive applications, such as ATMs and personal banking apps on mobile phones, etc.

Entering passwords by users is the weakest point in the chain of encrypting passwords and authenticating users [1, 2, 6]. Many existing shoulder-surfing resistant methods e.g., Convex Hull Click (CHC) [7], EvoPass [8], S3APS [9], [10], [11], [12] etc., focused on increasing the difficulty of disambiguating users' input to guess the passwords. Current shoulder-surfing resistant schemes typically achieve a higher level of security at the cost of reduced usability [1], such as long login time [6] as observed in Convex Hull Click [7], Déjà Vu [13], [14], and [15]. Some techniques, e.g., EvoPass [8] and [15] are not effective for an attacker with a recording device. Some approaches are quite complicated e.g., [11, 12, 16], and require extensive training and practice. Another common limitation is that these methods typically do not support traditional passwords, although they are still the most commonly used authentication method across many applications and devices.

In this study, we proposed and evaluated a shoulder-surfing resistant password scheme embedded in traditional passwords with a flat learning curve. It mitigates both shoulder-surfing and video recording attacks, and meanwhile keeps the advantages of traditional passwords, such as faster authentication speed, high user familiarity, and prevalent usage across applications and devices.

2. Related work

Existing shoulder-surfing resistant passwords are categorized and discussed below.

2.1. Graphical schemes

Graphical passwords use images or shapes instead of characters for better memorability [17]. However, a common limitation of graphical passwords is that they are more vulnerable to shoulder-surfing attacks [2, 5, 9, 14, 16, 18]. Some graphical passwords schemes were developed to resolve the problem. EvoPass [8] is an evolvable graphical password authentication scheme. It transforms password images into sketches and gradually

URI: https://hdl.handle.net/10125/71481
978-0-9981331-4-0

degrades them to provide less and less visual information to increase the difficulty to guess the pass sketches. However, it may not be effective for shoulder-surfing attacks with cameras. With the Convex Hull Click (CHC) scheme [7], users first identify their password icons. During the authentication procedure, users need to recognize their password icons among a much larger number of distracting icons. Instead of clicking on those password icons, users click within the convex hull of their password icons. It does not require users to click directly on their password icons, which makes the technique shoulder-surfing resistant. The triangle scheme proposed by Sobrado and Birget [19] is similar to CHC. To be authenticated, users need to find three of the password icons and click inside the invisible triangle created by them. Sobrado and Birget [19] also introduced the movable frame scheme, which requires users to move a password object to line up with another two password objects. Other special geometric configurations can also be used to determine the location the user needs to click, for example, the intersection of two invisible lines formed by four password icons [19]. Por et al. [11] proposed a shoulder-surfing resistant graphical password based on digraph substitution rules. They use the locations of pre-selected images to determine the locations of the password images based on several rules. For example, if two pre-selected images appear diagonal to each other in a grid of images, the row of the first image is the row for the password image, and the column of the second pre-selected image is the column for the password image. PairPassChar (PPC) also use similar rules to determine the icons to click on [16]. The method proposed by [12] requires users to remember three types of objects and to do different interactions on the screen based on complex rules, which can be challenging for users. A common drawback of those methods is that they require users to repeat the procedure to identify the right images or the right points/areas on an image or to move the password icons to the right locations (as in [19]) for several rounds, which increases the time they take for authentication. In fact, Abdullah et al. [20] evaluated 12 graphical password schemes and found 11 were considered as inefficient.

2.2. Textual-graphical schemes

Some schemes are both textual and graphical. The method proposed by Chen et al. [10] is based on both texts and colors. In the registration phase, a user sets a textual password and picks a color as the pass-color. In the login phrase, the system presents a wheel with eight equally-sized sections and each section has multiple characters on it. Around the wheel, there are eight color arcs. The user needs to rotate the wheel multiple times so that each character in the passwords is within the arc of the right color. TricolorPairPassChar (TPPC) is also color-based [16]. Users need to follow complex rules related to both the locations and the colors of characters in a large grid to determine the right characters in a password. Remembering all the rules can increase users' cognitive load. The pair-based authentication scheme proposed in [21] uses a pair of pre-selected letters in a grid to determine the location of a letter in a password. One pre-selected letter is to determine the row and the other is used to select the column. The hybrid textual authentication scheme in [21] uses pairs of colors to represent the location of the password characters in a grid. Users need to remember the numbers represented by different colors, which could increase users' memory burden [10]. The idea of S3APS [9] is similar to the triangle scheme [19] and CHC [7]. The major difference is that S3APS presents text to the user instead of icons. It also requires multiple rounds of interaction from the user to select each character in the password, which can be inefficient [10]. Some textual-graphical passwords make it possible to enter the password with a keyboard. However, they do not solve the long login time issue related to graphical passwords. In addition, color-based schemes can be challenging for people with color deficiencies. Although this group of authentication methods is textual-graphic, they are very different from traditional passwords and do not preserve the advantages of the latter, such as fast authentication speed, high user familiarity, and prevalent usage across applications and devices.

2.3. Biometric methods

Biometric methods, such as fingerprint, Face ID, and retina scan, could provide a higher level of security at the expense of increased hardware and software costs [2]. In addition, a device needs to have access to the biometric data of the user for authentication. For example, users must register their fingerprints before they can be used for authentication. Therefore, biometric methods cannot be used without storing the biometric data first, which can cause additional concerns on privacy and security, especially on public devices, such as lab computers and bank ATMs, etc. Gesture dynamics were used in [22] for continuous user authentication. DooDB [23] is also based on the dynamics of drawing gestures, such as speed and acceleration. Behavioral biometrics, such as keystroke dynamics and gesture dynamics, do not need expensive hardware, but introduces privacy issues [24].

2.4. Haptic-based techniques

Malek et al. [14] developed a haptic-based graphical password against shoulder-surfing attacks. Users need to draw a secret pattern on a grid and press harder for certain strokes in the pattern. Attackers won't be able to observe whether the pressure was applied while draws the strokes. In addition to input pressure, vibration is also used for authentication. With TictocPIN [25], users are informed through vibrations and simulated vibration sound. The Phone Lock is a PIN entry system [26] based on haptic cues. Users can enter a PIN using auditory or tactile stimuli. In [27], passwords are encoded as a sequence of vibration patterns to prevent shoulder-surfing attacks. VibraPass [28] was designed for ATM authentication using tactile feedback provided by the users' own mobile devices to determine what to enter. For example, when users' mobile phone vibrates, they enter a false character, if not, a correct one in the password. H4Plock [29] also used vibration cues. Haptic-based methods have special requirements for hardware, such as sensors for pressure and electric motors for vibration, which may limit their usage.

2.5. Extra hardware

Some techniques rely on extra hardware. Xside [30] allows users to enter a password using both the front and the back of a smartphone. EyePassword [1] enables gaze-based typing for password entry to make it difficult for an attacker to glean the password. Eye trackers were also used in [31-34]. Pass-thought [35] is an authentication scheme based on the Brain-Computer Interface technology. The extra hardware requirements limit the adaption of those techniques on regular devices, such as ATMs.

Some common challenges of existing techniques include 1) many anti-shoulder-surfing mechanisms increase the noise for the observer to make it more difficult to disambiguate a user' input, which usually also require more interactions from the user for authentication [1], and require a long time for authentication; 2) existing techniques are very different from traditional textual passwords, and they are not compatible with the latter despite their popularity; 3) some shoulder-surfing resistance schemes require additional hardware or software.

3. Proposed scheme

Textual passwords are still the most popular authentication methods. None of the techniques mentioned in section 2 solves the shoulder-surfing problem and keeps the authentication procedure of the traditional passwords. To fill the void, a shoulder-surfing resistant scheme embedded in traditional textual passwords was proposed as in Figure 1.

When a password field is on focus, a pattern shows up in the password field as a hint (referred to as hint pattern hereinafter) as in Figure 1 to tell a user how to enter a password. The user needs to enter characters at 'O's but skip those at 'X's. The "…" at the end of the pattern means there could be more characters in the password but was not included in the pattern. If a password is shorter than the pattern, the user can stop after finishing the password.

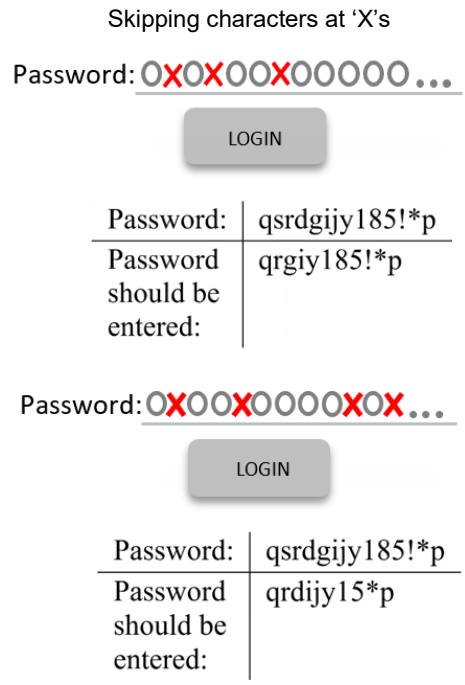


Figure 1. Proposed authentication scheme

The proposed scheme asks users to skip 2-4 randomly selected characters in a password in order to against shoulder-surfing attacks. Since a password is entered partially, an observer cannot steal the full-length password even if the input procedure was recorded. During password entry, the characters to be skipped are randomly selected. As a result, when an attacker tries to log into the system, the chance that the same hint pattern will be shown is low. In fact, there are 495 different hint patterns to skip 4 characters in a 12-character password. Moreover, we make sure the system does not repeat the same hint pattern within several consecutive attempts. Each time the password text field is clicked and becomes on focus, it is recorded as one authentication attempt. Incorrect attempts will be recorded to prevent an attacker from trying to find the same pattern that has observed. To prevent guessing attacks, including brute-

force attacks, our method employs a lock out policy to block a user who fails to enter the correct password after several attempts. For example, if a user enters wrong passwords for five times in a row, an email for two-factor authentication will be sent to the owner's email account to notice him/her the suspicious authentication attempts. The allowed number of attempts and the number of the characters to be skipped can be determined by the user.

When two characters are skipped, if an attacker observed an authentication procedure and obtained the rest of the password, there are 95 possibilities for each of the skipped character (26 lower case letters, 26 upper case letters, 10 digits, and 33 special characters). The attacker could have to guess up to 9025 (95*95) times to get the correct password. Similarly, with four omissions, attackers could have to guess up to 95^4 times. According to Kwon and Hong [25], 625 possibilities could be considered large enough to deter brute-force attacks. With only skipping two characters, our number is far above 625.

A partial password challenges users with a subset of characters from a full password [36]. Users are required to enter randomly selected characters at specific positions, such as the second, third, and sixth characters from their passwords [36]. Although our design also requires users to enter a subset of their passwords, it has some unique features: 1) To enter the letter at specific positions as in partial passwords, e.g., the second, third and sixth characters in a password, users have to recall both the characters and the positions, which is very challenging. With our design, a pattern hint is provided in the password field to tell the user to skip some characters while they are entering their passwords. Entered and skipped characters are marked with dots the same way as traditional passwords do (Figure 2(b)). Since skipping is embedded in the flow of entering a password, users only need to skip a character when they see an 'X' and they do not need to count the position number of the 'X'. Compared to recalling a character at a specific position, our design requires a lower cognitive load. 2) Partial passwords usually challenge the user with two or three characters [36]. Users only need to enter two or three characters, which is vulnerable to brute-force attacks. With our design, even after skipping some characters, the password length will still be much longer than two or three characters. For example, if the initial password has 12 characters and three of them are skipped, the password still has nine characters. It is still more brute-force attack resistant than partial passwords with two or three characters. 3) The proposed scheme is embedded in a traditional password, it preserves the benefits of the latter, such as user familiarity, and prevalent usage across different applications and devices. Besides, previous research on partial passwords, such as [36-38], did not evaluate the usability and user perceptions of partial passwords in their studies, and there is little academic research on partial passwords despite their usage in the industry [36, 37]. We want to fill the void in this study.

According to [6], shoulder-surfing attacks can be divided into three types: 1) attacks with naked eyes only, 2) recording the authentication procedure once, and 3) recording the authentication procedure more than once. Our design focuses on the first two types of attacks, and the third type is out of the scope of this study. In other words, our method is more suitable for security-sensitive but occasionally used applications, such as online banking accounts. Our method could be an add-on feature for traditional passwords, and users can enable it when they feel they are being observed or recorded, such as in a public place with surveillance cameras or while withdrawing money from ATMs.

(a) A hint pattern to skip three characters appears when the password field is on focus

(b) Entered and skipped characters are marked with dots

Figure 2. Hint patterns during password entry

4. Evaluation

We conducted a controlled laboratory experiment with a within-subject design to compare the proposed scheme with traditional passwords.

4.1. Participants

30 (13 female and 17 male) students from a university in the United States participated in this study. 12 were younger than 20 years old, 13 between 20 and 25 years old, 3 between 26 and 30 years old, and 2 were over 30 years old. They received a $10 gift card for participating in the study.

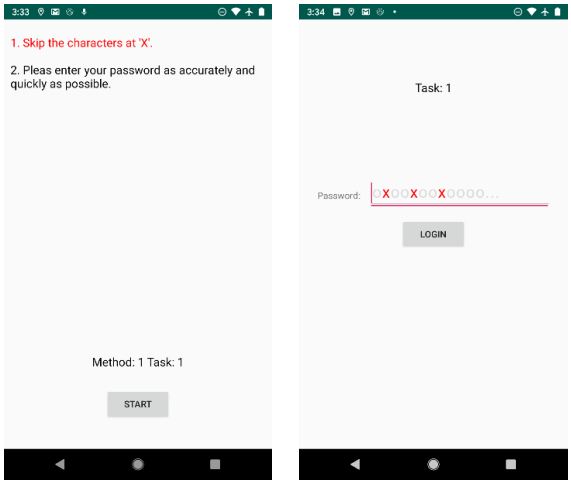
4.2. Apparatus

The proposed scheme was implemented in Java using Android Studio. The app was installed on a Google Pixel Phone with the 7.1.1 Android OS and a

5.0-inch AMOLED Full HD Touchscreen. The default QWERTY keyboard was used to enter passwords during the study.

4.3. Experiment tasks

Participants were required to enter a password they created for 10 times in each of the four task conditions, namely entering the regular password as they usually do, skipping 2 characters in the password, skipping 3 characters, and skipping 4 characters (referred as Regular, Skipping 2, Skipping 3, and Skipping 4 conditions hereinafter). There were 40 tasks in total. A sample task is shown in Figure 3. In figure 3(b), a participant clicked the password field, and the hint pattern to skip three characters appeared in the password field. The participant needed to enter his/her password while skipping the character at 'X's.



(a) (b)

Figure 3. An experiment task

4.4. Independent and dependent measures

The independent variable is the four password entry conditions, namely Regular, Skipping 2, Skipping 3, and Skipping 4.

The dependent variables are password entry speed, accuracy, and user perceptions. When the "START" button (Figure 3(a)) was clicked, the system recorded the time as the starting time for the task. When the "LOGIN" button was clicked (Figure 3(b)), the time was recorded as the completing time for the task.

7-point Likert scale questions were created to assess user perceptions, including "Acceptance", "Perceived Security", "Shoulder-Surfing Resistance", "Camera-Recording Resistance", "Guessing-Attack Resistance", "Ease of Use", "Efficiency", and "Overall Satisfaction". The questionnaire items are presented in Table 1.

Table 1. Questionnaire items

Factors	**Items (1 = "Strongly Disagree" and 7 = "Strongly Agree")**
Acceptance	I am likely to choose this method for security-sensitive applications, such as online banking, when in a public place.
Perceived Security	This method makes me feel safe to enter my passwords for security-sensitive applications, such as online banking, in a public place.
Shoulder-Surfing Resistance	I think this method resists shoulder-surfing attacks.
Camera-Recording Resistance	I believe this method resists camera-recording attacks.
Guessing-Attack Resistance	I think this method resists guessing attacks.
Ease of Use	I think the method was easy to use to enter a password.
Efficiency	I was able to enter my password quickly using this method.
Overall Satisfaction	Overall, I am satisfied with this password entry method.

4.5. Procedure

After signing a consent form, participants completed a demographic questionnaire. Then, they were required to create a password for the study. According to the commonly used guidelines, passwords should have at least eight characters with a mixture of upper and lower case letters, digits [19], and special characters [39]. We required participants to include at least 12 characters in their passwords. As a result, after skipping four characters, the rest of the passwords would still meet the eight-character length requirement. We also asked participants to use mixed upper- and lower-case letters, digits, and special characters. After creating the passwords, participants went through a training session to learn how to use the proposed scheme to skip 2, 3, and 4 characters while typing their passwords. After they felt comfortable with the proposed scheme, the experiment would start. Participants sat in a chair when they did the tasks. They could take breaks as they liked between tasks. The order of the four task conditions was counterbalanced with a Latin-square design.

After finishing the tasks, participants answered a questionnaire for user perceptions. Guessing attacks and shoulder-surfing attacks were explained to them. To make sure participants understand shoulder-surfing attacks, the following sketches as in Figure 4 were used to explain the concepts before they answer the questionnaire.

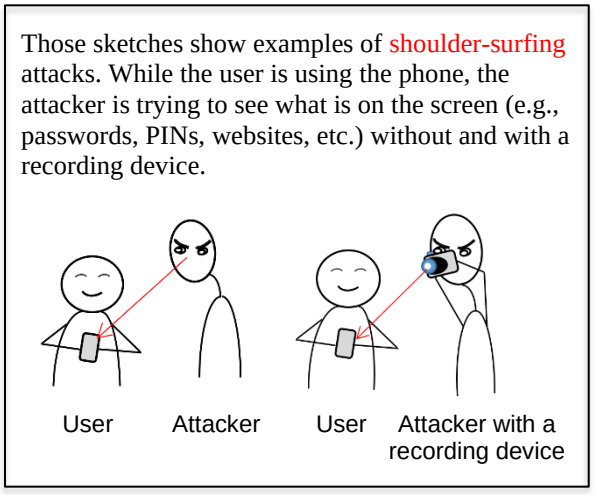


Figure 4. Sketches of shoulder-surfing attacks

5. Results

5.1. Password entry speed

The password entry speed of the four conditions was measured by "Task Completion Time". The means of the "Task Completion Time" for the four conditions are in Figure 5. The Repeated measures ANOVA results show that there were significant differences among the four conditions in "Task Completion Time" ($F_{(1.90, 55.10)} = 54.19$, $p < 0.001$) with Greenhouse–Geisser correction for sphericity violation. The regular condition took significantly less time than the other three conditions ($p < 0.001$). Skipping 2 was also faster than the other conditions ($p < 0.001$). There was no significant difference between Skipping 3 and Skipping 4.

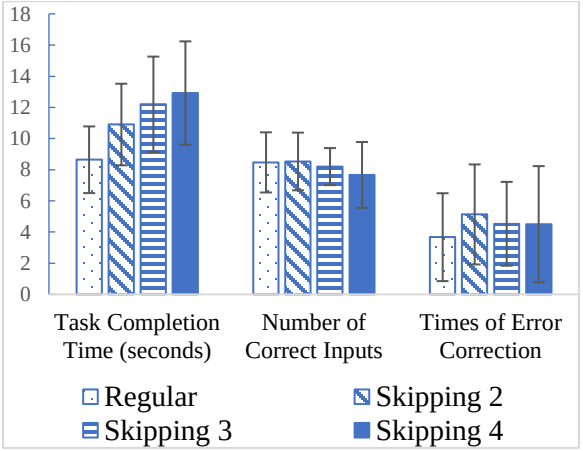


Figure 5. Task Completion Time, Number of Correct Inputs, and Times of Error Correction of four conditions

Compared to the Regular condition, Skipping 2 required additional 2.26 seconds. Skipping 3 required additional 3.56 seconds and Skipping 4 needed additional 4.28 seconds. Overall, the average additional time to skip one character was 1.13 seconds.

5.2. Password entry accuracy

The password entry accuracy of the four conditions was measured by the "Number of Correct Inputs" for 10 tasks and also the "Times of Error Correction" during the authentication procedure as in Figure 5. For example, if a participant thought a wrong character was entered and deleted all the characters had been entered and then re-typed the password, it is considered as one time of error correction. The larger the "Times of Error Correction", the more error-prone the condition is. Repeated measures ANOVA results show that there was no significant difference among the four conditions in "Number of Correct Inputs" ($F_{(3, 87)} = 2.20$, $p > 0.05$) and "Times of Error Correction" ($F_{(3, 87)} = 2.06$, $p > 0.05$).

5.3. User perceptions

The means and medians of the user perception factors ('1' = the lowest perceptions and '7' = the highest) are presented in Table 2. The main effects of conditions were all significant except for "Overall Satisfaction" (Table 2). The Greenhouse–Geisser method was used for sphericity violation correction.

Table 2. Means and medians of user perception

Factors	Measure	R	S2	S3	S4	Main effect
Acceptance	Mean	2.77	4.73	5.07	5.40	$F_{(1.83, 53.00)}$= 26.40 ***
	SD	1.68	1.39	1.36	1.65	
	Median	2.50	5.00	5.00	6.00	
Perceived Security	Mean	2.33	5.00	5.63	5.87	$F_{(2.38, 69.18)}$= 82.49 ***
	SD	1.18	1.46	1.27	1.31	
	Median	2.00	5.00	6.00	6.00	
Shoulder-Surfing Resistance	Mean	2.00	5.10	5.70	6.20	$F_{(1.86, 54.12)}$= 115.10 ***
	SD	1.31	1.35	1.09	1.06	
	Median	2.00	5.00	6.00	7.00	
Camera-Recording Resistance	Mean	1.73	4.60	5.33	5.87	$F_{(2.04, 59.27)}$= 95.85 ***
	SD	1.26	1.65	1.37	1.48	
	Median	1.00	5.00	5.50	6.00	
Guessing-Attack Resistance	Mean	1.87	4.70	5.43	5.73	$F_{(1.94, 56.33)}$= 88.38***
	SD	1.25	1.51	1.41	1.28	
	Median	2.00	5.00	5.50	6.00	
Ease of Use	Mean	6.23	4.37	3.73	3.37	$F_{(2.04, 59.09)}$= 29.83***
	SD	1.65	1.38	1.64	2.01	
	Median	7.00	5.00	3.50	3.00	
Efficiency	Mean	6.23	4.27	3.47	3.07	$F_{(1.45, 42.00)}$= 36.23***
	SD	1.76	1.39	1.59	1.95	
	Median	7.00	4.00	3.00	3.00	
Overall Satisfaction	Mean	4.17	4.80	4.27	4.37	$F_{(1.78, 51.60)}$= 1.19
	SD	1.82	1.27	1.55	1.87	
	Median	4.00	5.00	5.00	4.00	

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$
R: Regular; S2: Skipping 2; S3: Skipping 3; S4: Skipping 4

We also conducted pairwise comparisons when the main effects of conditions were significant as indicated in the last column in Table 2. The results were presented in Table 3.

For "Acceptance", "Perceived Security", "Shoulder-Surfing Resistance", "Camera-Recording Resistance", and "Guessing-Attack Resistance", the Regular condition received scores significantly lower than those of other conditions. However, for "Ease of Use" and "Efficiency", the scores of the Regular condition were significantly higher than those of the other conditions.

For "Perceived Security", "Shoulder-Surfing Resistance", "Camera-Recording Resistance", and "Guessing-Attack Resistance", Skipping 2 received lower scores comparing to Skipping 3 and Skipping 4. However, for "Ease of Use" and "Efficiency", the scores of the Skipping 2 condition were significantly higher than those of Skipping 3 and Skipping 4. Moreover, Skipping 3 and Skipping 4 did not have significant difference for all factors except for "Shoulder-Surfing Resistance" and "Camera-Recording Resistance". For "Overall Satisfaction", the main effect of conditions was not significant ($p > 0.05$), although Skipping 2 achieved the highest score.

Table 3. Pairwise comparisons of user perceptions

Factors	Pairwise comparison		
Acceptance	R < S1, S2, S3***	S2 < S4*	S2=S3 S3=S4
Perceived Security	R < S1, S2, S3***	S2 < S3** S2 < S4**	S3=S4
Shoulder-Surfing Resistance	R < S1, S2, S3***	S2 < S3*** S2 < S4***	S3<S4**
Camera-Recording Resistance	R < S1, S2, S3***	S2 < S3*** S2 < S4***	S3<S4**
Guessing-Attack Resistance	R < S1, S2, S3***	S2 < S3** S2 < S4**	S3=S4
Ease of Use	R > S1, S2, S3***	S2 > S3** S2 > S4***	S3=S4
Efficiency	R > S1, S2, S3***	S2 > S3*** S2 > S4***	S3=S4

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$
R: Regular; S2: Skipping 2; S3: Skipping 3; S4: Skipping 4
<: significantly smaller than; >: significantly larger than; =: no significant difference between

6. Discussion

The study results show that our scheme required marginal additional time compared to traditional passwords and achieved a similar level of accuracy. Overall, the average additional time to skip one character was 1.13 seconds, and most importantly skipping characters does not hurt password entry accuracy. Our scheme did not generate more errors in the final password strings entered for authentication. Meanwhile, it did not cause significantly more corrections during the authentication procedure. In fact, our method showed faster speed than existing shoulder-surfing resistant techniques, such as Convex Hull Click [7], Déjà Vu [13], [14], and [15]. Convex Hull Click Scheme took 72 seconds on average to authenticate a user [7]. Déjà Vu required 32 seconds. The method in [14] needed 78 seconds. Roth et al. [15] also found it took users about ten times longer to enter a PIN with their methods than with a regular keyboard. Those techniques against shoulder-surfing come at the price of longer authentication time. On the contrary, our method protects users from shoulder-surfing attacks without greatly sacrificing authentication speed. Furthermore, we observed a very flat learning curve during the study. Participants generally needed no more than ten minutes for the training session. In addition, these existing methods are quite different from and incompatible with traditional passwords. However, our method is embedded in traditional passwords, without requiring additional hardware or software. It retains the advantages of traditional textual passwords, such as fast authentication speed, user familiarity, and popularity. We believe it has the potential to be used widely for security-sensitive applications across different devices.

The mean of the Regular condition for "Acceptance" is 2.77 ('1' = the lowest perceptions and '7' = the highest), which means that participants did not want to use traditional passwords for security-sensitive applications, such as online banking, when in a public place. Participants showed significantly higher interest in our method, especially with skipping 4 characters, for security-sensitive applications.

Moreover, Skipping 2, Skipping 3, and Skipping 4 received 5.10, 5.70, and 6.20 for "Shoulder-surfing Resistant", while the score for the Regular condition was only 2.00. It seems the more characters skipped the more secure the participants felt. We see similar trends for "Perceived Security", "Camera-recording Resistance", and "Guessing-attack Resistance".

We also see an obvious tradeoff between usability and security in Tables 2 and 3. Although skipping more characters could increase security, it also decreased the scores for "Ease of Use" and "Efficiency". For "Overall Satisfaction", although the main effect of conditions was not significant, "Skipping 2" achieved the highest score. Probably skipping two characters balanced the tradeoff best between security and usability among all conditions. It is noteworthy that we did not mean to replace traditional passwords with the proposed scheme in any situation. Our method could be an add-on feature for traditional passwords, and users can enable it when they feel they are being observed or recorded, such as in

a public place with surveillance cameras or while withdrawing money from ATMs.

There are some limitations in this study. Our scheme showed advantages against shoulder-surfing attacks with and without camera recording, but it is not effective for repeated observations. As a result, our scheme cannot resist shoulder-surfing attacks conducted by close friends or family members who have the chance to observe the victim multiple times. Nevertheless, for security-sensitive applications, such as banking account and ATMs, users usually do not enter passwords repeatedly in a short period of time. Thus, we believe the chance for a stranger to observe the authentication procedure repeatedly could be low. One way to fight against repeated observation is to make sure hint patterns for consecutive authentication attempts have a least one common character to skip. However, it may still not be effective enough for attackers who can observe the victim many times. Second, we did not address the memorability issue of textual password in this study. We would like to explore more in those aspects in our future study.

7. Conclusion

In this study, we designed and empirically evaluated a shoulder-surfing resistant scheme embedded in traditional passwords. When a password field is on focus, a pattern shows up on the screen in the password field as a hint to tell the user how to enter a password. The user needs to skip some randomly selected characters so that attackers will not be able to observe the whole password. Many existing shoulder-surfing techniques, such as graphical passwords, are quite different from traditional passwords and require users to learn new authentication schemes. Different from those techniques, our method has a flat learning curve and can be seamlessly embedded in traditional passwords. As a result, it retains the benefits of traditional passwords, such as fast authentication speed, user familiarity, and the prevalent usage across different applications and devices, and meanwhile against shoulder-surfing and recording attacks. Participants showed interest in using it for security-sensitive techniques.

References

[1] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing Shoulder-Surfing by Using Gaze-based Password Entry," in *Proceedings of the 3rd Symposium on Usable Privacy and Security*, 2007: ACM, pp. 13-19.

[2] F. Tari, A. Ozok, and S. H. Holden, "A Comparison of Perceived and Real Shoulder-Surfing Risks between Alphanumeric and Graphical Passwords," in *Proceedings of the Second Symposium on Usable Privacy and Security*, 2006: ACM, pp. 56-66.

[3] M. A. S. Gokhale and V. S. Waghmare, "The Shoulder Surfing Resistant Graphical Password Authentication Technique," *Procedia Computer Science*, vol. 79, pp. 490-498, 2016.

[4] M. Eiband, M. Khamis, E. Von Zezschwitz, H. Hussmann, and F. Alt, "Understanding Shoulder Surfing in the Wild: Stories from Users and Observers," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017: ACM, pp. 4254-4265.

[5] A. H. Lashkari, S. Farmand, D. Zakaria, O. Bin, and D. Saleh, "Shoulder Surfing Attack in Graphical Password Authentication," *arXiv preprint arXiv:0912.0951*, 2009.

[6] H.-M. Sun, S.-T. Chen, J.-H. Yeh, and C.-Y. Cheng, "A Shoulder Surfing Resistant Graphical Authentication System," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 2, pp. 180-193, 2018.

[7] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme," in *Proceedings of the Working Conference on Advanced Visual Interfaces*, 2006: ACM, pp. 177-184.

[8] X. Yu, Z. Wang, Y. Li, L. Li, W. T. Zhu, and L. Song, "EvoPass: Evolvable Graphical Password against Shoulder-Surfing Attacks," *Computers & Security*, vol. 70, pp. 179-198, 2017.

[9] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, 2007, vol. 2: IEEE, pp. 467-472.

[10] Y.-L. Chen, W.-C. Ku, Y.-C. Yeh, and D.-M. Liao, "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme," in *2013 International Symposium on Next-Generation Electronics*, 2013: IEEE, pp. 161-164.

[11] L. Y. Por, C. S. Ku, A. Islam, and T. F. Ang, "Graphical Password: Prevent Shoulder-Surfing Attack Using Digraph Substitution Rules," *Frontiers of Computer Science*, vol. 11, no. 6, pp. 1098-1108, 2017.

[12] G. W. Bin, S. Safdar, R. Akbar, and S. Subramanian, "Graphical Authentication based on Anti-Shoulder Surfing Mechanism," in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, 2018: ACM, p. 20.

[13] R. Dhamija and A. Perrig, "Deja Vu-A User Study: Using Images for Authentication," in *Proceedings of the USENIX Security Symposium*, 2000, vol. 9, pp. 4-4.

[14] B. Malek, M. Orozco, and A. El Saddik, "Novel Shoulder-Surfing Resistant Haptic-Based Graphical Password," in *Proc. EuroHaptics*, 2006, vol. 6, pp. 1-6.

[15] V. Roth, K. Richter, and R. Freidinger, "A PIN-Entry Method Resilient Against Shoulder Surfing," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, 2004, pp. 236-245.

[16] K. Rao and S. Yalamanchili, "Novel Shoulder-Surfing Resistant Authentication Schemes Using Text-Graphical Passwords," *International Journal of Information and Network Security*, vol. 1, no. 3, p. 163, 2012.

[17] H. Gao, W. Jia, F. Ye, and L. Ma, "A Survey on the Use of Graphical Passwords In Security," *JSW*, vol. 8, no. 7, pp. 1678-1698, 2013.
[18] X. Suo, Y. Zhu, and G. S. Owen, "Graphical Passwords: A Survey," in *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC'05)*, 2005: IEEE, pp. 463-472.
[19] L. Sobrado and J.-C. Birget, "Graphical Passwords," *The Rutgers Scholar, an Electronic Bulletin for Undergraduate Research*, vol. 4, pp. 12-18, 2002.
[20] M. D. H. Abdullah, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge based Authentication Technique," in *Proceedings of the 2008 Second Asia International Conference on Modelling & Simulation (AMS)*, 2008: IEEE, pp. 396-403.
[21] M. Sreelatha, M. Shashi, M. Anirudh, M. S. Ahamer, and V. M. Kumar, "Authentication Schemes for Session Passwords Using Color and Images," *International Journal of Network Security & Its Applications*, vol. 3, no. 3, pp. 111-119, 2011.
[22] L. Zhou, Y. Kang, D. Zhang, and J. Lai, "Harmonized Authentication based on Thumbstroke Dynamics on Touch Screen Mobile Phones," *Decision Support Systems*, vol. 92, pp. 14-24, DEC 2016 2016, doi: 10.1016/j.dss.2016.09.007.
[23] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "The Doodb Graphical Password Database: Data Analysis and Benchmark Results," *IEEE Access*, vol. 1, pp. 596-605, 2013.
[24] M. Nauman, T. Ali, and A. Rauf, "Using Trusted Computing for Privacy Preserving Keystroke-Based Authentication in Smartphones," *Telecommunication Systems*, vol. 52, no. 4, pp. 2149-2161, 2013.
[25] T. Kwon and J. Hong, "Analysis and Improvement of a Pin-Entry Method Resilient to Shoulder-Surfing and Recording Attacks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 278-292, 2015.
[26] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices," in *Proceedings of the fifth International Conference on Tangible, Embedded, and Embodied Interaction*, 2010, pp. 197-200.
[27] A. Bianchi, I. Oakley, and D. S. Kwon, "The Secure Haptic Keypad: a Tactile Password System," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 1089-1092.
[28] A. De Luca, E. Von Zezschwitz, and H. Hußmann, "Vibrapass: Secure Authentication based on Shared Lies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2009, pp. 913-916.
[29] A. Ali, A. J. Aviv, and R. Kuber, "Developing and Evaluating a Gestural and Tactile Mobile Interface to Support User Authentication," in *Proceedings of the IConference 2016*, 2016.
[30] A. De Luca *et al.*, "Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 2937-2946.
[31] A. Maeder, C. Fookes, and S. Sridharan, "Gaze based User Authentication for Personal Computer Applications," in *Proceedings of the 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004.*, 2004: IEEE, pp. 727-730.
[32] V. Rajanna, A. H. Malla, R. A. Bhagat, and T. Hammond, "DyGazePass: A Gaze Gesture-based Dynamic Authentication System to Counter Shoulder Surfing and Video Analysis Attacks," in *Proceedings of the 2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, 2018: IEEE, pp. 1-8.
[33] V. Rajanna, S. Polsley, P. Taele, and T. Hammond, "A Gaze Gesture-based User Authentication System to Counter Shoulder-Surfing Attacks," in *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 2017: ACM, pp. 1978-1986.
[34] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010: ACM, pp. 1107-1110.
[35] J. Thorpe, P. C. Van Oorschot, and A. Somayaji, "Pass-Thoughts: Authenticating with Our Minds," in *Proceedings of the 2005 Workshop on New Security Paradigms*, 2005, pp. 45-56.
[36] D. Aspinall and M. Just, ""Give Me Letters 2, 3 and 6!": Partial Password Implementations and Attacks," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, 2013: Springer, pp. 126-143.
[37] T. Mourouzis, M. Wojcik, and N. Komninos, "On the Security Evaluation of Partial Password Implementations," *arXiv preprint arXiv:1701.00104*, 2016.
[38] P. I. Sethumadhavan, "Partial Password Authentication using Vector Decomposition," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 7, pp. 381-386, 2018.
[39] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 102-127, 2005.