Hindawi
Security and Communication Networks
Volume 2021, Article ID 6653076, 11 pages
https://doi.org/10.1155/2021/6653076

Research Article

A Camouflage Text-Based Password Approach for Mobile Devices against Shoulder-Surfing Attack

Suliman A. Alsuhibany

Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia

Correspondence should be addressed to Suliman A. Alsuhibany; salsuhibany@qu.edu.sa

Received 31 October 2020; Revised 4 January 2021; Accepted 7 January 2021; Published 20 January 2021

Academic Editor: Ximeng Liu

Authentication in mobile devices is inherently vulnerable to attacks and has the weakness of being susceptible to shoulder-surfing attack. Shoulder-surfing attack is a type of attack that uses direct observation techniques such as looking over someone's shoulder to get information. This paper aims to introduce a novel way of concealing the password within a contingent of randomly selected entries. In particular, the traditional password concept where what you input is what you get is redefined by proposing the camouflage characters approach. Based on this approach, three defensive techniques are introduced for mobile devices. By using an Android platform, the introduced techniques are implemented. Experimental studies are conducted in order to evaluate both security and usability perspectives. The empirical results showed that the proposed approach is reasonably resistant against shoulder-surfing attacks and usable for participants. Moreover, it is possible to choose very short passwords, while insuring that the password remains hidden amongst a large number of key presses. Based on the achieved results, the proposed approach is recommended to be a new avenue in the field of security to produce very simple and yet very complicated passwords, to be observed by the attacker, at the same time.

1. Introduction

Nowadays, the use of mobile devices has increased at an unanticipated rate. In particular, the landscape of mobile devices, such as smart phones, has significantly changed; that is, mobile devices are now used not only for calling and sending messages but also for several services such as e-mail, social network, and web surfing [1]. In order to perform a trusted communication between these services and the user, the user authentication, which is the process of confirming an alleged identity, is required. This authentication process requires the user to be as accurate as possible; otherwise, the entry will fail. This presents a significant challenge to users and designers of a secure system alike.

The user authentication is broadly categorized into three classes [2]: token-based authentication, which is based on something one has such as traditional keys to the doors; biometric-based authentication, which is based on a physiological or behavioral characteristic such as fingerprint and keystroke dynamic; knowledge-based authentication, which is based on something one knows such as text-based passwords. The use of text-based passwords is almost the popular method of the knowledge-based authentication class. However, a number of drawbacks of using text-based password have been raised; for example, a short text-based password can be easily guessed, while long passwords are often hard to remember [3]. To overcome this weakness, a graphical password has been proposed [4] as an alternative to the text-based password, where a user can remember pictures better than text.

Moreover, a wide range of research efforts suggest authentication protocols and techniques such as IllusionPIN (IPIN) [5] and audio and haptic entry systems [6]. The main aim of these methods was to find a way of safeguarding the password entry. Interestingly, both methods, i.e., text-based and graphical passwords, are vulnerable to shoulder-surfing attacks [7], which is a type of attack that uses direct observation techniques such as looking over someone's

shoulder to get information. A recent study in [8] stated that text-based passwords created on mobile devices are substantially weaker against shoulder-surfing attacks. Despite the fact that concealing the output on the screen would minimally prevent the attack, an attacker can observe chosen keys on the keyboard.

In this paper, the canonical key entry mechanism is reconsidered. The impetus was to establish a scheme that allows easy, safe, and shoulder-browsing resistant password entry. Typically, a keystroke means only one thing which is the stored value of that key. We argue for a respecification of key functions in login systems. Specifically, the proposed approach uses two master keys: enable and disable. The former enables entering the actual password, whereas the latter disables the actual password. Assigning these functions to the keys adds another layer to the process of selecting a password. To enter a password, firstly, the user enters any number of random camouflage characters. Then, these camouflage characters are followed by the enable key, and this key should be followed by the password. Finally, the user enters the disable key followed by any number of random camouflage characters. This allows a flexible password entry in terms of choosing a simple entry if needed or choosing a complex combination of characters to hide the actual password. Furthermore, the proposed approach solves one of the main weaknesses of alphanumeric passwords, i.e., having to choose a simple password to remember due to the limited capacity of the human memory (e.g., Yan et al. research work [9]). Since this paper proposes an approach against shoulder-surfing attacks, the brute-forcing attack is beyond the scope of this paper in case of applying one digit as a password. Furthermore, although this approach has been introduced in Alsuhibany's work [10,11] for shared spaces such as tabletops and pattern-based passwords, respectively, this approach is extended here in this paper for creating traditional text-based passwords for mobile devices.

Based on the proposed approach, three defensive techniques are designed and implemented for mobile devices. The first technique allows the user to specify the length of camouflage characters in which the activation and deactivation keys are reflected by a number of characters and have the same length. The second technique allows the user to specify the length of camouflage characters of both keys but with various lengths. The third technique allows the user to specify only one character as an activation key and another as a deactivation key. For testing these techniques, we developed an Android application. Then, we conducted an empirical experiment for evaluating the security and usability aspects. The accomplished results showed a statistical significance difference between the three defensive techniques. In particular, the third technique was the best in terms of security and usability aspects.

The rest of the paper is organized as follows. Section 2 reviews related works. The proposed approach is explained in Section 3. Section 4 shows the experimental study. The results are presented in Section 5 and discussed in Section 6. Section 7 concludes the paper.

2. Related Works

Researchers have been trying to boost the usability and security of authentication schemes by minimizing the vulnerability of such systems to shoulder-surfing attacks [12]. For example, Lee et al. [13] proposed a bimodal Personal Identification Number (PIN) entry method using an audio channel. Their proposed framework is different from other methods in which the audio channel only transmits the minimal required data needed for the authentication while most of the information that the user needs is transmitted via the visual channel. A study by Park et al. [14] developed a puzzle authentication method that uses a grid-based authentication scheme in which the user has to pick 4 out of 16 panels and 4 out of 16 positions. Furthermore, Kwon and Hong [15] claim that their black-and-white PIN scheme shows good results in resisting camera-based recording attacks. Moreover, Roth et al. presented in [12] cognitive trapdoor games that make shoulder-surfing attacks harder for a criminal to obtain PINs. Further, Lee and Nam proposed in [16] a method that uses a random mapping between the PIN digits and alphabets given as challenges to the user. Furthermore, the issue of the shoulder-surfing attack on authentication systems is addressed in [5] by proposing the IllusionPIN (IPIN) method, which operates on touchscreen devices. A novel PIN-based authentication mechanism for smartphones called ColorSnakes which uses fake paths on a grid of numbers to disguise user input is introduced in [17]. The results of this study reveal that this mechanism could be used as an additional authentication mechanism alongside current mechanisms. Another novel mechanism is presented in [18] called SwiPIN that allows input of traditional PINs using simple touch gestures like up or down. In addition, DRAW-A-PIN is proposed in [19] that supports the use of PINs. Similarly, a new online finger-drawn PIN authentication method is introduced in [20] which allows a user draw a PIN on a touch interface with their finger. Although the results indicated that a further study is needed to enhance the introduced method. In Binbeshr et al's study [21], a systematic review for PIN-entry methods is presented. The results showed that an evaluation framework needs to be addressed.

Besides, GazeTouchPIN proposed in [22] that combines gaze and touch input as a new secure authentication approach for mobile devices. Also, Kumar et al. presented in [23] a Gaze-Based password entry approach in order to prevent the shoulder-surfing attack. A survey on gaze-based security applications was carried out in [24] that discussed a set of opportunities as well as challenges. Likewise, the gaze-based application is reviewed in [25] and classified into three categories: authentication, privacy, and gaze monitoring. An investigation for estimating the gaze of possible attackers is carried out in [26]. To support the gaze-based sensing application, a generalized framework is developed in [27].

In terms of the convenience, Yan et al. [9] stated that many of the deficiencies of textual passwords arise from the limitations of human memory. Moreover, the usability and shoulder-surfing vulnerability of text-based password entry on mobile devices are investigated in [28]. This study

provided a set of insights for the security-aware design of on-screen keyboards. Furthermore, evaluations of a number of mobile devices have been performed in [6]. A study by Florencio et al. [29] reported the results of a large-scale study of text-based password. These results include password strength and length of the chosen password. Furthermore, the password strength and user behavior are investigated in [30] using a large-scale study. Besides, the results of a user survey are discussed in [31] in which actual stories of shoulder surfing on mobile devices from both users and observers are investigated. Likewise, in 2019, a new approach to mask text passwords by distorting them by using graphical filters was proposed; that is, once the password is distorted, it can be difficult to be observed by attackers as they cannot mentally reverse the distortions [32]. Additionally, a hybrid scheme, which combines the advantage aspects of graphical-based and text-based methods, is proposed in [33]. Also, the characters of the text-based password are modified in [34] in order to provide higher entropy levels. A hybrid approach that exploits the advantages of textual and graphical passwords is introduced in [35]. A shoulder-surfing resistance scheme embedded in the textual password is proposed in [36]. The results of this study are promising in terms of both accuracy level and time.

A new one-time password method is proposed by Huang et al. [37]. In this method, they used a two-factor password system that relies on time and sequence numbers. Moreover, Aratani and Kanai [38] proposed an authentication method that used two types of channels. They used numbers, colors, and input from the device, such as auditory information or vibrations.

Additionally, the CoverPad proposed by Yan et al. [39] for the password entry on touchscreen mobile devices. The EyePassword approach that mitigates the issue of shoulder-surfing attacks is presented in [23]. This approach has empirically shown that it requires marginal additional time for any keyboard. A study in [40] examined the feasibility of such smudge attacks on touch screen.

A recent study by Pais et al. [11] introduced a camouflage pattern technique as a shoulder-surfing resistance approach for mobile devices. Despite the camouflage notion is applied in this study, it is implemented only on the pattern password method which is an alternative authentication approach for the password-based authentication scheme. Accordingly, applying camouflage notion on the password-based authentication might enhance its resistance against shoulder-surfing attacks.

The proposed approach in this paper, therefore, focuses on redefining the concept of alphanumeric passwords. What differentiates our approach is that the sequence of entries is not necessary. In fact, the main strength of this novel approach is that it deliberately marginalizes this sequencing requirement in passwords. Since, in the shared spaces such as tabletops, in one way or another, there is the trade-off between security and usability, and the proposed approach takes into account the compromise between the usability and security. Thus, the contributions of our paper are as follows: (1) introducing a camouflage text-based password approach for mobile devices against the shoulder-surfing attack; (2) based on this approach, three defensive techniques are designed, implemented, and empirically evaluated.

3. Camouflage Text-Based Password Approach: An Overview

The camouflage text-based password approach basically redefines the traditional password concept where what you input is what you get. Specifically, the proposed approach uses two master keys: enable (i.e., the activation key) and disable (i.e., the deactivation key). The former enables entering the actual password, whereas the latter disables the actual password. Assigning these functions to keys adds another layer to the process of selecting a password. To enter a password, firstly, the user can enter any number of random Camouflage Characters (CC). Then, these camouflage characters are followed by an Activation Key (AK), and this activation key should be followed by the password. Finally, the user enters a Deactivation Key (DK) followed by any number of random CCs. Figure 1 summarizes this mechanism.

This mechanism allows flexible password entry in terms of choosing a simple entry if needed or choosing a complex combination of characters to hide the actual password. Furthermore, the proposed approach solves one of the main weaknesses of alphanumeric passwords, i.e., having to choose a simple password to remember due to the limited capacity of the human memory (e.g., [9]). As stated previously, since this paper proposes an approach against shoulder-surfing attacks, the brute-forcing attack is beyond the scope of this paper in case of applying one digit as a password.

The initial version of this approach was established in [10]. In this paper, however, we extend this approach to be applicable for mobile devices by introducing three defensive techniques. The first technique allows the user to specify the same length of camouflage characters in which the activation and deactivation keys are reflected by a number of characters. The second technique allows the user to specify the length of camouflage characters of both keys but with various lengths. The third technique allows the user to specify only one character as an activation key and another as a deactivation key. In order to define precisely each one of these techniques, the following paragraphs explore these techniques, respectively. Figure 2 shows a screenshot from the first interface of the developed application.

In the first technique (Type 1), the camouflage characters contain the activation and deactivation keys. In particular, once the last character of the first camouflage characters set is written by the user, the keyboard becomes an active amount in which the password can be typed. Then, the second camouflage characters set, which reflect the deactivation key, should be written in a specific length like the first set. For example, when a user chooses "5" as a password and "4" as the length of camouflage characters, then the user can login to a system with "398157462." It is important to note that the length of camouflage characters is randomly chosen in the setting stage. Figure 2(b) illustrates the Type 1's

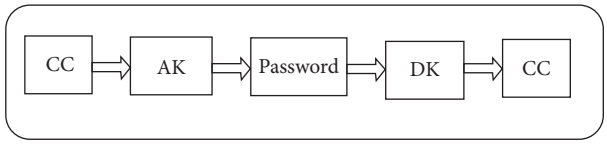

Figure 1: The general proposed authentication mechanism.

Figure 2: (a) A screenshot from the first interface of the developed application that shows the three techniques: types 1, 2, and 3. (b) Type 1's interface. (c) Type 2's interface. (d) Type 3's interface.

interface in which the user is asked to choose an ID, a password, and the length of camouflage characters and then asked to login to the system.

In the second technique (Type 2), the camouflage characters contain the activation and deactivation keys, but with a different length; that is, once the last character of the first camouflage characters is written by the user, the keyboard becomes active in which the password can be typed. Then, the second camouflage characters, which reflect the deactivation key, should be written in a specific length that is determined in the setting stage. For example, when a user chooses "55" as a password, "3" as the length of the first camouflage characters (i.e., activation key), and "5" as the length of the second camouflage characters (i.e., deactivation key), then the user can login to a system with "2215537881." It is important to note that the length of camouflage characters in this technique cannot be the same. Figure 2(c) illustrates the Type 2's interface in which the user is asked to

choose an ID, a password, the length of the activation key, and the length of the deactivation key and then asked to login to the system.

Finally, the third technique (Type 3) is different from the above described types in which the activation and deactivation keys are independent from the camouflage characters. Specifically, the user can choose three main elements: an activation key, a password, and a deactivation key. The activation and deactivation keys should be only one digit. Characters other than these elements will be counted as camouflage characters. For example, when a user chooses "555" as a password, "2" as the activation key, and "1" as the deactivation key, then the user can login to a system with "869425551335967", where the camouflage characters can be seen clearly before the activation key and after the deactivation key. Figure 2(d) illustrates the Type 3's interface in which the user is asked to choose an ID, a password, the activation key, and the deactivation key and then asked to login to the system.

Remarkably, Type 3 is comparable with our initial version in [10], and we will highlight this in the result section. Table 1 summarizes the functionality of these techniques.

These techniques are designed, implemented, and evaluated for mobile devices; that is, we developed an Android application which includes all aforementioned techniques. Then, we conducted an empirical experiment for evaluating the security and usability aspects. It is interesting to note that although there are other platforms that can be used for the evaluation purpose such as iOS, Windows Phone, and Symbian, the Android platform takes almost 50% share of the worldwide smart phone market [41].

As stated in [42], the password strength is a combination of length, complexity, and unpredictability. Therefore, in the proposed approach, the camouflage characters can generally give the illusion of added complexity and length to a chosen password, whereas the activation and deactivation keys can provide the unpredictability concept. This could have broad implications for a wide range of authentication contexts in general and password entry techniques in particular.

4. Experimental Study

The aim of this experimental study is to evaluate the security and usability of the proposed defensive techniques on mobile devices. The following describes specific details of the experimental setup and procedure.

4.1. Setup. The experiment involves a number of subjects, thus the design, ID, password, participants, and system are described in this section.

4.1.1. Design. We performed a within-subject lab study to compare the usability and shoulder-surfing resistance aspects of the proposed defensive techniques. In our study, we focus on the effects of design features of each technique on the efficiency, effectiveness, satisfaction, and shoulder-surfing resistance.

Table 1: Summarizing the proposed defense techniques.

Defense technique	Keys	
	Activation	Deactivation
Type 1	Included in the camouflage characters with the same length	
Type 2	Included in the camouflage characters with different lengths	
Type 3	Independent from the camouflage characters, and each has only one digit	

4.1.2. ID, Password, and Keys. The ID, password, and keys (i.e., activation and deactivation keys) are chosen by the users for each smart phone and defensive technique. The main reason for this is to make the experiment as realistic as possible in terms of creating an ID and a password. Moreover, in order to make the comparison of entry time for all types more meaningful, the chosen password and keys should not exceed 15 digits. This stage may potentially cause some confusion on the part of participants as they have to choose three different elements with three different functions.

4.1.3. Participants. We recruited thirty five participants (4 females and 31 males, aged 21–29 years) from our campus population. The majority of participants had a computer science background.

4.1.4. System. We developed and implemented an Android application for password enrolment and login according to the description in Section 3. This application then was installed on two Android OS smart phones which are as follows: HTC Smartphone and Samsung Galaxy Tab 3.

4.1.5. Survey. We deployed an online survey using the Google form. The survey consists of 15 items ranked on a 5-point Likert scale: strongly agree, agree, neither agree nor disagree, disagree, and strongly disagree. These 15 items of the survey result in four scales measuring user satisfaction [43] as follows: perceived usefulness of the technique in completing the given tasks (SysUse), perceived quality of displayed information (InfoQual), interface elements (InterQual), and overall satisfaction with the technique (Overall), that is, each user is asked to complete the survey after using a defensive technique type. Therefore, this survey reflects the user satisfaction and had some demographic questions.

4.2. Procedure. The way that we ran the experiment is described, i.e., instructions to subject, procedures of both the usability and shoulder surfing, and collected data.

4.2.1. Instruction. Subjects were instructed that there are two smart phones that will be utilized. In each one, there are three different defensive techniques that need to be evaluated for both the usability and shoulder-surfing aspects. The

subjects were instructed that there are two sessions: the first session is for evaluating the usability, and the second session is for evaluating shoulder surfing. For the usability session, subjects were instructed to choose an ID and a password as well as the activation and deactivation keys. Subjects were instructed to give a feedback regarding each defensive technique through a given survey. For the shoulder-surfing session, subjects were instructed about the danger of shoulder surfing in public places. Subjects were instructed that they will act as shoulder surfers, while the experimenter will play the victim and enter a password for the defensive technique.

4.2.2. Usability Experiment Procedure. We assessed usability of the proposed defensive technique with a consideration of quantitative and qualitative metrics. A defensive scheme's efficiency is measured by the entry time required for login; the effectiveness is assessed with the login success rate for entering a password. To measure the entry time, the developed application records the entry time automatically. In addition to these quantitative usability results, qualitative usability results are collected via a survey, which provides qualitative data on user's satisfaction based on participants rating on a 5-point Likert scale, as explained previously. Thus, we derive the following hypothesis for the usability aspect:

(i) $\mathbf{H_1}$: significant difference exists in the entry time between the three different defensive techniques

(ii) $\mathbf{H_2}$: significant difference exists in the login success rate between the three different defensive techniques

The experiment began with an introductory session where participants were given a brief explanation of the proposed defensive techniques. Printed information was also supplied to support the briefings. This was followed by a short demo to show how the system works, and a quick hands-on demo took place to ensure that the participants had some experience using the developed application prototype before they engage with the actual task.

For all defensive techniques, the participants were instructed at the beginning to perform the following task:

(i) Become familiar with the defensive techniques by allowing the participants to create their own passwords. Then, they practice logging to the application several times. In order to ensure a consistent amount of training, each participant was allowed approximately 10 minutes (this amount of time was found to be adequate during a pilot study that we conducted).

Once the training period was over, the participants were instructed to perform the following tasks:

(ii) Participants were instructed to login using their own passwords for each smart phone and defensive technique.

(iii) Participants were instructed that there are three login attempts per password. The first successful login in these three attempts will be counted as a successful login.

(iv) Participants were instructed to complete an online survey regarding the defensive technique they just used.

4.2.3. Shoulder-Surfing Experiment Procedure. The usability experiment was followed by the shoulder-surfing experiment. We assessed the defensive technique's susceptibility to shoulder surfing with the success rate of the shoulder surfer, i.e., how well the typed password could be reproduced. In order to accomplish this, the proposed methodology in [44] is utilized where a binary metric approach is used to measure the shoulder-surfing success; that is, "1" if the participant entered the correct password within three attempts and "0" otherwise. Therefore, we derive the following hypothesis:

(i) $\mathbf{H_3}$: a significant difference exists in the success rate of the shoulder surfer between the three different defensive techniques

Furthermore, we followed the common approach of having participants act as shoulder surfers [7, 28, 45–48]. The experimenter acted as the victim to the shoulder-surfing attack throughout this experiment. The reason for having just the experimenter being the victim is to reduce the inconsistency bias produced by two different person's login skills from affecting the results. Furthermore, the experimenter underwent sufficient training to ensure constant speed in writing the passwords. The training proved sufficient as the experimenter managed to conduct the login procedure without any failed attempts. It is important to note that the experimenter was not trying to cover up the device (i.e., the smartphone or tablet) or applying any defense technique other than the one being tested. The purpose of having this scenario is to have a tight control so that the victim has no other protection method, despite the fact that in real life situations smartphone or tablet users might tilt the screen to avoid being seen. For shoulder surfers (i.e., participants), they could choose to stand in right behind the victim or behind the left or right shoulder. After entering a password by the experimenter, each participant tried to enter the observed passwords on the device, with a maximum of three attempts per password.

4.2.4. Collected Data. The entry time, login success rate, users' satisfaction, and shoulder-surfing success rate were recorded.

5. Results

In the experimental study, all participants successfully completed their task. We first discuss in Section 5.1 the usability results of the proposed defensive techniques including testing the hypothesis with respect to the efficiency and effectiveness and testing the satisfaction of the participants. We then discuss the shoulder-surfing results of the proposed defensive techniques mainly testing the hypothesis of the shoulder-surfing success rate.

5.1. Usability Results. This section shows the results of testing the efficiency, effectiveness, and satisfaction of the proposed defensive techniques.

5.1.1. Entry Time. The average time needed to enter the password (this indicates both the password, activation, and deactivation keys) in each of three defensive techniques is shown in Figure 3. From the HTC and Tab bars, we see that Type 2 took longer time than Types 1 and 3. Also, Type 1 took longer time than Type 3. This indicates that there are implications to the applied defensive technique, but we will discuss this more precisely below. In all types, the smartphone (HTC) took more time than the tablet (Tab).

The statistical significance of the time entry will be discussed now. Table 2 compares the results of both the HTC and Tab in all defensive techniques with respect to the time needed to enter the password. For this, we provide average (Avg.), standard deviation (SD), maximum (Max), and minimum (Min).

By using the HTC smartphone, we find the following with respect to the average time; it took 20.8 seconds in Type 1, 23.2 seconds in Type 2, and 18.5 seconds in Type 3. An one-way analysis of variance yielded a significant difference among the three proposed techniques ($F = 27.8$ and $P < 0.0005$) in which the F value assesses whether the expected values of a quantitative variable within several predefined groups that differ from each other, whereas P refers to the probability of getting a result at least as extreme as the one that was actually observed. This is added in the paper. On the other hand, using the tablet, we find the following: it took 18.8 seconds in Type 1, 21.5 seconds in Type 2, and 16.9 seconds in Type 3. An one-way analysis of variance yielded a significant difference among the three proposed techniques ($F = 25.3$ and $P < 0.0005$). Hence, the hypothesis H_1, where a significant difference exists in the entry time between the three different defensive techniques, was supported.

5.1.2. Login Success Rate. The login success rate is the average of successful logins over all attempts of one participant. Table 3 shows the mean values as well as the SD per technique for both the HTC smartphone and tablet.

For the HTC smartphone, an one-way analysis of variance yielded a significant difference that exists in the login success rate between all defensive techniques ($F = 4.68$ and $P < 0.1$). For the tablet, an one-way analysis of variance yielded a significant difference that exists in the login success rate between all defensive techniques ($F = 4.50$ and $P < 0.1$). These results supported our hypothesis 2.

5.1.3. Satisfaction. The survey consists of 15 items, which result in four scales measuring user satisfaction, as we explained previously. Table 4 shows the satisfaction results of each technique.

An one-way analysis of the variance test indicates a significant difference in SysUse in all techniques ($F = 28.56$ and $P < 0.001$). Furthermore, a t-test yields a result of $t = 3.94$ and $P < 0.001$, indicating that the difference between SysUse in defensive technique 1 and SysUse in defensive technique 2 is definitely statistically significant. For InfoQual scale, an one-way analysis of the variance test indicates a significant difference in all techniques ($F = 22.98$ and $P < 0.001$). For the InterQual scale, an one-way analysis of the variance test indicates a significant difference in all techniques ($F = 13.60$ and $P < 0.001$). Finally, for the Overall scale, an one-way analysis of the variance test indicates a significant difference in all techniques ($F = 59.40$ and $P < 0.001$). Furthermore, Type 3 shows more satisfaction than other types.

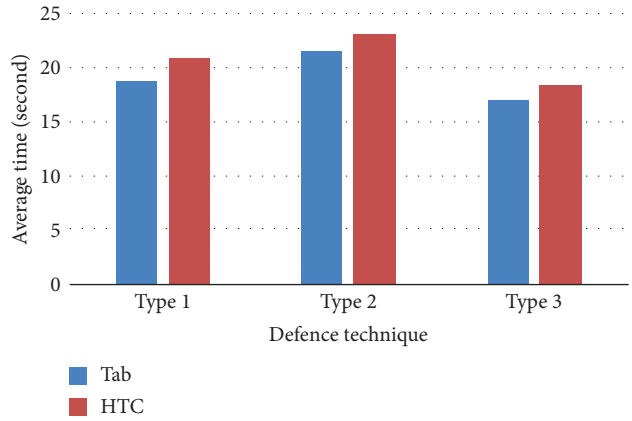

Figure 3: The average time (in seconds) to enter a password in each defensive technique.

5.2. Shoulder-Surfing Results. The shoulder-surfing experiment was performed after the usability experiment. Therefore, this section shows the results of the shoulder-surfing success rate.

The difference in how passwords are entered in all defensive techniques leads to the use of, as mentioned previously, the proposed methodology in [44] as a fair and comparable distance metric between the entered and correct password. Table 5 summarizes the total percentage of correctly guessed passwords for each technique.

A statistical test is conducted for both HTC and Tab devices. In particular, an one-way analysis of the variance test indicates that a significant difference exists in the success rate of the shoulder surfer between all defensive techniques using the HTC device ($F = 2.67$ and $P < 0.01$). For Tab device, an one-way analysis of the variance test indicates that a significant difference exists in the success rate of the shoulder surfer between all defensive techniques ($F = 5.82$ and $P < 0.01$). The results above show that our hypothesis 3 is supported. Moreover, it can be clearly observed that Type 3 in both devices is more resistant to the shoulder-surfing attack than other types.

6. Discussion

The accuracy obtained with our experiment indicates that using the camouflage characters can be a defensive mechanism against the shoulder-surfing attack as well as a usable method.

Table 2: Summarizing the results of the time needed to enter the password.

Defensive technique	Device	Total time (seconds)			
		Avg.	SD	Max	Min
Type 1	HTC	20.8	3.25	26.8	15.4
	Tab	18.8	3.25	27.23	12.69
Type 2	HTC	23.2	2.10	27.60	19.80
	Tab	21.5	2.70	32.15	18.30
Type 3	HTC	18.5	2.51	22.70	12.83
	Tab	17.06	2.08	21.20	13.40

Table 3: Summarizing the results of the login success rate.

Defensive technique	Device	Login success rate	
		Mean	SD
Type 1	HTC	0.764	0.430
	Tab	0.794	0.410
Type 2	HTC	0.647	0.485
	Tab	0.705	0.462
Type 3	HTC	0.941	0.238
	Tab	0.970	0.171

Table 4: Summarizing the results of the satisfaction.

Defensive technique	Scale	Satisfaction scale rate	
		Mean	SD
Type 1	SysUse	3.55	0.824
	InfoQual	3.853	0.610
	InterQual	3.588	0.892
	Overall	3.558	0.560
Type 2	SysUse	2.73	0.898
	InfoQual	3.147	0.744
	InterQual	3.529	0.506
	Overall	2.647	0.950
Type 3	SysUse	4.147	0.557
	InfoQual	4.235	0.654
	InterQual	4.264	0.447
	Overall	4.500	0.507

In particular, using the proposed approach showed a significant difference among the three proposed techniques; that is, the Type 3 showed the best in the usability experiment with short password entry times, high typing accuracy, and satisfaction. Moreover, this type also showed the best in the success rate of the shoulder surfer with 8.8% compared to 29.4% and 44.1% for types 1 and 2, respectively. It might be worth to note that no hidden factors are included in the proposed techniques, and for example, Bianchi et al. [6] proposed the audio and haptic feedback that can only be available to users, as it cannot be obtained by attackers. However, the proposed camouflage characters approach in general is a challenge for attackers, as shown in our experiments. Moreover, a diversification in using the proposed techniques, along with a better understanding of how they are used, reduces the possibility of deducing the real password. Furthermore, the possible key to gain the advantage of Type 3 may be its functionality, as shown in Table 1, that is, the activation and deactivation keys are independent from the camouflage characters and more importantly, each key has only one digit. Despite this advantage, there might be some cognitive load that needs to be exerted by the person inputting the password as they need to pay attention to which keys are assigned to which roles. However, this might not be a downside as much as a strong feature of the technique since every login now is unique.

It is interesting to note that as stated in [28], the different virtual keywords used on HTC and Tablet devices can affect password entry usability and shoulder-surfing vulnerability; and this can be seen clearly in Tables 2–5.

It seems that the second defensive technique (i.e., Type 2) is extracted from the first defensive technique (i.e., Type 1). Specifically, most of their results whether in the usability aspects or in the success rate of the shoulder surfer are close

Table 5: Summarizing the results of the shoulder-surfing success rate.

Device	% of correctly guessed passwords for each technique		
	Type 1 (%)	Type 2 (%)	Type 3 (%)
HTC	17.6	26.4	5.8
Tab	29.4	44.1	8.8

Table 6: Comparing our results with most related works.

Study	Usability		Security
	Entry time (sec.)	Login success rate	Shoulder-surfing success rate
[12]	23–67	NA	NA
[38]	12.8–14.4	NA	NA
[15]	15.3	NA	NA
[16]	5.8–6.8	3.7–6.7%	NA
[23]	10	NA	NA
[22]	10.8	9.55%	10.42–68%
[17]	6.8–3.1	NA	10.5%
[18]	3.66	97%	16%
[39]	10.3–11.7	98.3%	NA
[19]	6.12	98.51%	85%
[20]	NA	NA	12.83%
Our study	20.8^{*}, 23.2^{**}, 18.5^{***} 18.8^{+}, 21.5^{++}, 17.06^{+++}	76%*, 64%**, 94%*** $79\%^{+}$, $70\%^{++}$, 97^{+++}	17.6%*, 26.4%**, 5.8%*** $29.4\%^{+}$, $44.1\%^{++}$, $8.8\%^{+++}$

HTC: Type 1^{*}, Type 2^{**}, Type 3^{***} | Tab: Type 1^{+}, Type 2^{++}, Type 3^{+++}.

to each other. For example, in Table 4, the mean satisfaction scale rate results of Types 1 and 2 are very close. Therefore, a t-test yields a result of $t = 0.33$ and $p = 0.739$, indicating that no statistically significant difference was found between the Overall in Type 1 and the Overall in Type 2, although there was a significant difference in all types, as mentioned previously. Also, for the success rate of the shoulder surfer, a t-test yields a result of $t = 0.87$ and $P = 0.388$, indicating that no statistically significant difference was found in the success rate of the shoulder surfer between Types 1 and 2 using the HTC device. The same result is for Tab devices, where a t-test yields a result of $t = -1.25$ and $P = 0.214$, indicating that no statistically significant difference was found in the success rate of the shoulder surfer between Types 1 and 2.

Similarly, the impact of the screen size on the usability and security aspects [28] can be reflected by the achieved results. For example, the average time needed to enter the password in the HTC device was more than in the Tab device for all types, as shown in Figure 2. Furthermore, regardless of the defensive technique used, the screen size of the tablet device might have an effect on the vulnerability to the shoulder-surfing attack, as shown in Table 5. These results can support the results in [49]. The solution of this may be, additionally to use a defensive technique, increasing the attention of users while using devices with a large screen size. Although creating text-based passwords on mobile devices takes significantly longer [8], we believe that the proposed defensive techniques can be suggested as a way to easy password entry for mobile users. Moreover, the implications for the design of privacy protection mechanisms due to the shoulder-surfing attack in the real world have been investigated in [31]. Thus, the proposed defensive techniques can be a protection mechanism against this attack. Table 6 compares our results with most related works in terms of security and usability aspects.

It is interesting to note that using the proposed defensive techniques for mobile devices can allow unlocking the mobile with only two key presses, which are the activation key and password (when not being watched), or using as many clicks an user wants when being otherwise without the need to have a separate password for each case. However, on the other side of the coin, it might be slightly complex at the early stage of usage, as users need to get used to it.

Moreover, the proposed defensive techniques provide the ability for designers to manipulate access rights without the need for any further implementations of protocols as the password entry now is not what it used to be. One of the options that can be utilized in this scheme is assigning access rights to the master keys. This allows mobile devices users, for example, to keep their sensitive data safe on their devices; that is, when the master keys are used in a certain sequence, access to the phone is only limited to making calls.

7. Conclusion and Future Work

The concept of alphanumeric passwords for mobile devices is redefined in this paper by proposing the camouflage character scheme. Based on this scheme, three defensive techniques are introduced. By using an Android platform, the introduced techniques are implemented. In order to evaluate the usability and security levels of the proposed approach, two experimental studies were conducted. The results of this evaluation showed that the Type 3 of the proposed defensive techniques demonstrated higher ratings

in the usability experiments with short password entry times, high typing accuracy, and high scores on its satisfaction survey. In addition, the Type 3 proved also to be the best in resisting shoulder-surfing attacks. Moreover, the results obtained with the Type 3 show the possibility of choosing very short passwords, while insuring that the password remains hidden amongst a large number of key presses. This makes passwords tend to be very long without requiring any extra memory load.

Based on the achieved results, the proposed approach is recommended to be a new avenue in the field of security to produce very simple and yet very complicated passwords, to be observed by the attacker, at the same time. The proposed defensive techniques might have an advantage against smudge and thermal attacks. However, it would be investigated as one of our future works.

Data Availability

The data used to support the findings of this study are available upon request to the author.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The author would like to thank Qassim University for supporting this research work.

References

[1] A. Porter Felt and D. Wagner, "Phishing on mobile devices," in *Proceedings of the Web 2.0 Security & Privacy*, California, Oakland, May 2011.

[2] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.

[3] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: a survey," in *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC'05)*, p. 10, IEEE, San Juan, PR, USA, December 2005.

[4] G. E. Blonder, "Graphical passwords," US Patent 5559961, 1996.

[5] A. Papadopoulos, T. Nguyen, E. Durmus, and N. Memon, "Illusionpin: shoulder-surfing resistant authentication using hybrid images," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2875–2889, 2017.

[6] 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*, pp. 197–200, ACM, Funchal, Madeira, Portugal, January 2011.

[7] 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*, pp. 56–66, ACM, Pittsburgh, PA, USA, July 2006.

[8] W. Melicher, D. Kurilova, S. M. Segreti et al., "Usability and security of text passwords on mobile devices," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 527–539, ACM, San Jose, CA, USA, May 2016.

[9] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: empirical results," *IEEE Security & Privacy Magazine*, vol. 2, no. 5, pp. 25–31, 2004.

[10] S. Alsuhibany and S. Almutiri, "Making PIN and password entry secure against shoulder surfing using camouflage characters," *International Journal of Computer Science and Information Security*, vol. 14, no. 7, 2016.

[11] S. A. Alsuhibany, "Usability and shoulder surfing vulnerability of pattern passwords on mobile devices using camouflage patterns," *Journal of Ambient Intelligence and Humanized Computing*, vol. 111 pages, 2019.

[12] 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*, pp. 236–245, ACM, Washington, DC, USA, October 2004.

[13] M.-K. Lee, H. Nam, and D. K. Kim, "Secure bimodal PIN-entry method using audio signals," *Computers & Security*, vol. 56, pp. 140–150, 2016.

[14] M. Park, Y. Kita, K. Aburada, and N. Okazaki, "Proposal of a puzzle authentication method with shoulder-surfing attack resistance," in *Proceedings of the 2014 17Th International Conference On Network-Based Information Systems*, pp. 495–500, IEEE, Salerno, Italy, September 2014.

[15] 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.

[16] M.-K. Lee and H. Nam, "Secure and usable pin-entry method with shoulder-surfing resistance," in *Proceedings of the International Conference on Human-Computer Interaction*, pp. 745–748, Springer, Berlin, Germany, July 2013.

[17] J. Gugenheimer, A. De Luca, H. Hess, S. Karg, D. Wolf, and E. Rukzio, "Colorsnakes: using colored decoys to secure authentication in sensitive contexts," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pp. 274–283, Copenhagen Denmark, August 2015.

[18] E. Von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, "Swipin: fast and secure pin-entry on smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 1403–1406, Seoul, South Korea, April 2015.

[19] T. V. Nguyen, N. Sae-Bae, and N. Memon, "DRAW-A-PIN: authentication using finger-drawn PIN on touch devices," *Computers & Security*, vol. 66pp. 115–128, May 2017.

[20] T. Van Nguyen, N. Sae-Bae, and N. Memon, "Finger-drawn pin authentication on touch devices," in *Proceedings of the IEEE International Conference on Image Processing (ICIP)*, pp. 5002–5006, IEEE, Paris, France, October 2014.

[21] F. Binbeshr, M. M. Kiah, L. Y. Por, and A. A. Zaidan, "A systematic review of PIN-entry methods resistant to shoulder-surfing attacks: computers & security," 2020.

[22] M. Khamis, M. Hassib, E. V. Zezschwitz, A. Bulling, and F. Alt, "GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication," in *Proceedings of the 19th ACM International Conference on Multimodal Interaction*, pp. 446–450, Glasgow, UK, November 2017.

[23] 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*, pp. 13–19, ACM, Pittsburgh, PA, USA, July 2007.

[24] C. Katsini, Y. Abdrabou, G. E. Raptis, M. Khamis, and F. Alt, "The role of eye gaze in security and privacy applications: survey and future HCI research directions," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–21, Honolulu, HI USA, April, 2020.

[25] C. Katsini, Y. Abdrabou, G. E. Raptis, M. Khamis, and F. Alt, "The role of eye gaze in security and privacy applications: survey and future HCI research directions," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–21, Honolulu, HI, USA, April 2020.

[26] A. Saad, D. H. Elkafrawy, S. Abdennadher, and S. Schneegass, "Are they actually looking? identifying smartphones shoulder surfing through gaze estimation," in *Proceedings of the ACM Symposium on Eye Tracking Research and Applications*, pp. 1–3, Stuttgart, Germany, June 2020.

[27] G. LAN, "GazeGraph: graph-based few-shot cognitive context sensing from human visual behavior," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, pp. 422–435, New York, NY, USA, November 2020.

[28] F. Schaub, R. Deyhle, and M. Weber, "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," in *Proceedings of the 11th international conference on mobile and ubiquitous multimedia*, p. 13, ACM, Ulm, Germany, December 2012.

[29] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*, pp. 657–666, ACM, May 2007.

[30] S. Komanduri, R. Shay, P. G. Kelley et al., "Of passwords and people: measuring the effect of password-composition policies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2595–2604, ACM, Vancouver, BC, Canada, May 2011.

[31] 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*, pp. 4254–4265, Denver, CO, USA, May 2017.

[32] M. Khamis, T. Seitz, L. Mertl, A. Nguyen, M. Schneller, and Z. Li, "Passquerade: improving error correction of text passwords on mobile devices by using graphic filters for password masking," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–8, Glasgow, Scotland, Uk, May 2019.

[33] S. Varshney, M. S. Umar, and A. Nazir, "A secure shoulder surfing resistant hybrid graphical user authentication scheme," *Cybernetics, Cognition and Machine Learning Applications*, Springer, in *Proceedings of the Cybernetics, Cognition and Machine Learning Applications*, pp. 79–87, November 2020.

[34] M. J. Dupuis, J. Shorb, J. Walker, F. B. Holt, and M. McIntosh, "Do you see what I see? The use of visual passwords for authentication," in *Proceedings of the 21st Annual Conference on Information Technology Education*, pp. 58–61, Fort Lauderdale, FL, USA, October 2020.

[35] J. K. Han, X. Bi, H. Kim, and S. S. Woo, "PassTag: a graphical-textual hybrid fallback authentication system," in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, pp. 60–72, Auckland, New Zeland, October 2020.

[36] J. Lai and E. Arko, "A shoulder-surfing resistant scheme embedded in traditional passwords," in *Proceedings of the 54th Hawaii International Conference on System Sciences*, p. 7144, Maui, HI, USA, January 202.

[37] Y. Huang, Z. Huang, H. Zhao, and X. Lai, "A new one-time password method," *IERI Procedia*, vol. 4, pp. 32–37, 2013.

[38] A. Aratani and A. Kanai, "Authentication method against shoulder-surfing attacks using secondary channel," in *Proceedings of the 2015 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 430-431, IEEE, Las Vegas, NV, USA, January 2015.

[39] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, pp. 37–48, Hangzhou, China, May 2013.

[40] S. L. Pais, P. S. Nikshita, S. N. Priyanka, and U. P. Tharunya, "Illusion PIN: tricking the eye to defeat shoulder surfing attack by using hybrid images," *Editorial Board*, vol. 9, no. 7, 2020.

[41] http://www.canalys.com/static/press_release/2011/canalys-press-release-010811-android-takes-almost-50-share-worldwide-smartphone-market_0.pdf.

[42] "Choosing and protecting passwords," 2021, https://us-cert.cisa.gov/ncas/tips/ST04-002.

[43] J. R. Lewis, "IBM computer usability satisfaction questionnaires: psychometric evaluation and instructions for use," *International Journal of Human-Computer Interaction*, vol. 7, no. 1, pp. 57–78, 1995.

[44] F. Schaub, M. Walch, B. Könings, and M. Weber, "Exploring the design space of graphical passwords on smartphones," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, p. 11, ACM, Newcastle, UK, July 2013.

[45] P. Dunphy, A. P. Heiner, and N. Asokan, "A closer look at recognition-based graphical passwords on mobile devices," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, p. 3, ACM, Washington, DC, USA, July 2010.

[46] D. Kim, P. Dunphy, P. Briggs et al., "Multi-touch authentication on tabletops," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1093–1102, ACM, Atlanta Georgia USA, April 2010.

[47] J. Nicholson, *Design of a Multi-Touch Shoulder Surfing Resilient Graphical password, B. Sc in Information Systems*, Newcastle University, Newcastle, UK, 2009.

[48] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, p. 6, ACM, Pittsburgh, PA, USA, July 2011.

[49] M. Anwar and A. Imran, "A comparative study of graphical and alphanumeric passwords for mobile device authentication," in *Proceedings of the MAICS*, pp. 13–18, Greensboro, NC, USA, April 2015.