Computer Systems Science & Engineering
DOI:10.32604/csse.2022.018563
Article

Tech Science Press

Vibration-Based Pattern Password Approach for Visually Impaired People

Suliman A. Alsuhibany*

Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia
*Corresponding Author: Suliman A. Alsuhibany. Email: salsuhibany@qu.edu.sa
Received: 12 March 2021; Accepted: 01 May 2021

Abstract: The pattern password method is amongst the most attractive authentication methods and involves drawing a pattern; this is seen as easier than typing a password. However, since people with visual impairments have been increasing their usage of smart devices, this method is inaccessible for them as it requires them to select points on the touch screen. Therefore, this paper exploits the haptic technology by introducing a vibration-based pattern password approach in which the vibration feedback plays an important role. This approach allows visually impaired people to use a pattern password through two developed vibration feedback: pulses, which are counted by the user, and duration, which has to be estimated by the user. In order to make the proposed approach capable to prevent shoulder-surfing attacks, a camouflage pattern approach is applied. An experimental study is conducted to evaluate the proposed approach, the results of which show that the vibration pulses feedback is usable and resistant to shoulder-surfing attacks.

Keywords: Information security; authentication; vibration-based pattern password; visually impaired people; shoulder-surfing attacks

1 Introduction

Due to the technological revolution, people have become reliant on their smart devices in everyday life. Moreover, many people store personal and sensitive information on them making security a major concern. This therefore leads to the need to take into account the authentication process, which is a security technique [1]. There are many authentication approaches proposed in the literature. One of these approaches is a graphical password [2] that has been developed as an alternative to the text password authentication system. Moreover, it uses predefined items from a set of images or certain geometric shapes in a specific order [3].

Using a graphical password is a memory task because it relies on the user remembering and entering a password. Furthermore, it is a part of a recall-based system, which consists of two types: pure recall-based and cued recall-based, and recognition-based system. Regarding pure recall-based and cued recall-based systems, the former is a blank canvas or grid where users create a password, whereas the latter is where users select a specific location on images they have previously chosen during the password creation process. For the recognition-based system, the user selects a set of images during the password creation process and then they are asked to choose the same images for the login process.

The pattern authentication system is defined as one of graphical authentication systems [1–3] and is used to simplify the verification process. That is, pattern authentication system has a total of 389 112 possible patterns, which is more than 10,000 possible 4 digit Personal Identification Numbers (PIN) codes [4]. Moreover, its secret information appears to be a drawing which can be easily memorized by users. Therefore, this system can be classified as a pure recall-based system.

The shoulder-surfing attack is one of the most important security issues that developers have been unable yet to find a usable and secure solution to [1,4,5]. This is in spite of the effortlessness of this type of attack which is carried out by stealing information while looking over a victim's shoulder, and by video recording or electronically capturing [6] the users' password when they use it. To make users more vulnerable to this type of attack, they tend to create simple passwords that they can easily remember.

People with visual impairments have been stated in The Lighthouse National Survey [7] as those who have low vision, or are blind in both eyes or in one of them and cannot read properly while wearing typical corrective lenses. Studies in Refs. [8,9] show that a remarkable number of people with visual impairments are not interested to protect their smartphones by applying an authentication method due to inaccessibility or inconvenience. In addition, a pattern password drawn on the screen is also inaccessible for people with visual impairments because it requires them to select points on the touch screen [10,11]. This, thus, shows the need for improving a pattern authentication system to be appropriate for people with visual impairments.

Therefore, our paper exploits the human-mobile interaction by focusing on haptic technology. This technology is used by people with visual impairment as a secondary form of accessing and understanding touchscreen. Moreover, the well-known example of this technology is the rumble in a game controller and the vibration in mobile devices. Hence, this paper proposes a vibration-based pattern password which allows people with visual impairments to protect their smartphones. In particular, we have developed two vibration feedbacks: (1) feedback through vibration pulses which are counted by the user, and (2) feedback through vibration duration which has to be estimated by the user. Furthermore, the proposed vibration-based pattern password enhances the security and protects against shoulder-surfing attacks by applying the camouflage pattern methodology [1]. The proposed approach is evaluated experimentally. The results of this evaluation show that this approach is usable for people with visual impairments and can help prevent shoulder-surfing attacks.

The remainder of this paper is structured as follows: Section 2 reviews the related work. Section 3 explains the vibration-based pattern password approach. Section 4 provides an overview of the camouflage pattern methodology. The experimental study is described in Section 5. The results are presented in Section 6 and discussed in Section 7. This paper is concluded in Section 8.

2 Related Works

To the best of the authors' knowledge, this study is the first to address the topic of adapting vibration-based pattern passwords for visually impaired people. Accordingly, this section highlights those studies which utilize the accessibility features and numerous approaches to protecting the privacy of people with visual impairments.

2.1 Accessibility Features of Smartphones

There are several accessibility features that make interaction with a touch-screen smartphone easy for the visually impaired. For example, for iOS smartphones the screen elements can be heard using the VoiceOver [12] and for Android smartphones TalkBack [13] can be used as a screen reader. Moreover, a virtual and physical Braille keyboard [14] can be connected to smartphones via Bluetooth. Some methods are proposed to solve smartphone usability issues regarding the interaction with the touch screen and entering data. For example, a speech recognition method is proposed in Azenkot et al. [15] as a main interaction

method for input. However, this proposal is susceptible to aural eavesdropping attacks in public spaces. A Braille recognizer method is proposed in Refs. [16,17] to identify touch gestures. Although there are some interesting results, this method does not have widespread use within the visually impaired community and it could make them more vulnerable to shoulder-surfing attacks.

A mobile pattern authentication method is proposed in Balaji et al. [10] for visually impaired users which provides a color and touch sensitive based dot pattern lock. The results of this study show that the proposed method is usable without any major access barriers. However, this study does not solve the low security issue of the used pattern method. A bend password is developed in Refs. [18,19] to reduce the vulnerability of attack while using the accessibility features (e.g., screen readers and screen magnifiers) for people with visual impairments. Furthermore, a study in Azenkot et al. [8] develops a PassChords method which is a non-visual authentication for blind smartphone users. Although this produces some interesting results, it does not prevent aural and visual eavesdropping.

2.2 Smart Devices Protection Approaches for People with Visual Impairments

The study in Hayes et al. [20] investigates how people with visual impairments protect their smart devices' privacy/security in daily life. The results show how they often work closely and cooperatively with their allies to protect their privacy and security. Another study in Haque et al. [21] demonstrates that people with visual impairments are more vulnerable to shoulder surfing attacks when entering passwords. A novel EarTouch approach is proposed in Wang et al. [22] which is a one-handed interaction technique that allows users to interact with a smartphone using their ears to perform gestures on the touchscreen. The results show that the proposed approach is socially acceptable and easy to use.

In Alnfiai et al. [23], a BraillePassword method is developed for people with visual impairments. This method minimizes the risk of observation or shoulder attacks without any extra fees for special hardware. Similarly, the impact of physical privacy, security and safety risks that may arise while interacting with their surrounding environment to people with visual impairments is explored in Ahmed [24]. Further, a password manager approach for visually impaired people called Unipass is designed and evaluated in Barbosa et al. [25], and the evaluation results showed the usability of this approach.

To understand the authentication methods used on mobile devices by people with visual impairments, an online survey is conducted in Faustino et al. [26]. The results of which provide insights for designing better authentication methods for such people.

Although these studies consider different prevention approaches against shoulder surfing attacks for the visually impaired, their formulations do not fit with the approach in this study.

2.3 Vibration for Touchscreen Accessibility

A comprehensive review of touchscreen accessibility is conducted in Grussenmeyer et al. [27]. Based on this study, several new research directions have been proposed. However, using the vibration mode for authenticating people with visual impairments has not yet been investigated. Moreover, to make Braille accessible on touchscreen, vibration feedback is proposed in Jayant et al. [28,29] which showed promising results. Besides, BlindLogin approach is proposed in Ho et al. [30]. This approach is compared in Schaub et al. [31] with other graphical password authentication systems for people with visual impairments. The initial results of this study showed that the BlindLogin approach is more memorable than others. However, this approach is just designed and developed as a proof of concept and also does not fit with the approach in this study. Schaub et al. [31] studied the key usability parameters that control rendering of haptically-perceivable graphical materials. The results of this study provided several guidelines for rendering visual graphical materials on touchscreen-based interfaces. Moreover, the contextual properties of touchscreen vibrations and how vibrations be used are

investigated in Tennison et al. [32]. The results of this study empirically established a range of vibration effects that are distinguishable by users.

3 Vibration-Based Authentication Approach

This section provides an overview of the proposed approach and describes its length of vibration feedback and implementation.

3.1 An Overview

Generally, the smart phones have numerous feedbacks to the users such as a visual feedback by showing a clickable button, a sound feedback by hearing a selected ring and a vibration[1] feedback by vibrating the device. The vibration in mobile environment has been studied in terms of finding the optimal frequency level, e.g., Yim et al. [33]. For the visually impaired people, the vibration has been proposed as a solution to their inability to perceive their surroundings; for example it is proposed for helping them in the navigation systems [34]. However, it has not been yet investigated for authentication purpose. Therefore, this section explains the adaption of the proposed vibration technique for authenticating visually impaired people.

As we mentioned previously, although the pattern password method is amongst the most attractive authentication methods, it is inaccessible for people with visual impairments due to the impossibility of selecting points on the touch screen. Consequently, this paper focuses on the haptic technology which is used by people with visual impairments for accessing and understanding touch screens. The vibration in mobile devices is considered the most famous example of this technology. Thus, our paper improves the vibration-based technique in order to make the pattern password method convenient for people with visual impairments. The details are described in the following.

Nowadays, the vibration mode is one of important components in the mobile devices. That is, it is helpful to notify the users when the auditory and visual modalities are restricted due to, for example, environmental factor. Moreover, the vibration mode is used not only for signaling incoming call or text messages, but also for representing several sources like location-based services and games. However, it has not yet utilized for making the authentication appropriate for people with visual impairments. Therefore, the vibration-based technique is proposed.

The proposed technique is inspired by the Braille system[2], where blind people gain the ability to recognize the letters of the alphabet by using their sense of touch. Thus, this approach exploits this ability by assigning a unique vibration for each node on the unlock pattern grid. In particular, a unique vibration feedback is assigned for each pattern which allow the visually impaired people to recognize the patterns by using their sense of touch; for example, when a pattern is touched, a specific vibration feedback is given that will be discussed in the following section, as shown in Fig. 1.

Since the optimal vibration frequency level has been investigated previously in Yim et al. [33], the standard frequency level which is used in Android devices is utilized in our study. Accordingly, our study focuses on the uniqueness of the vibration feedback rather than the vibration frequency level. The proposed vibration feedback is discussed in the following section.

3.2 Pilot Study

The purpose of this pilot study is to understand what is the limit in terms of short vibration signal that human can reliably distinguish and to determine a distinguishable vibration signal for each pattern. The implementation, grid size, participants and length of vibration feedback are discussed in the following.

[1] The vibration is defined as a mechanical occurrence whereby vibrations take place on a fixed point.

[2] Braille is "a system of touch reading and writing for blind persons in which raised dots represent the letters of the alphabet" (https://brailleworks.com/braille-resources/history-of-braille/).

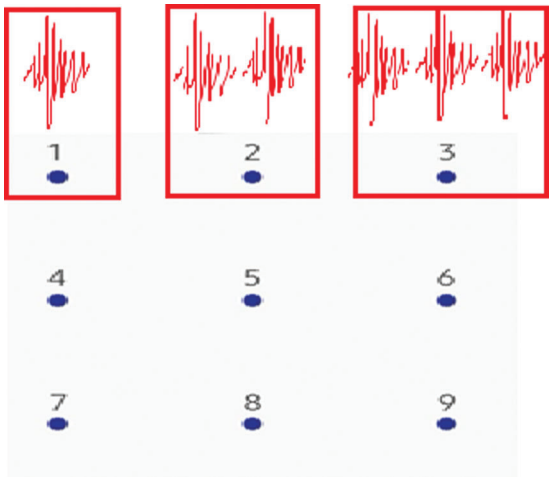

Figure 1: Illustration of the vibration time for 1, 2, and 3 patterns

3.2.1 Implementation

The Android operating system is utilized to implement the two types of the proposed approach using an Android Studio Development Environment (version 3.5.3). Although the proposed approach is implemented on an Android platform, the iOS application will be developed in one of our future works. This application is then installed on two Android OS smart phones (Samsung Galaxy s6 edge and Lenovo). Importantly, the screen size is identical on both the devices.

3.2.2 Grid Size

A grid size of 3 × 3 is used as shown in Fig. 1. The reason behind choosing this size is that a minimal impact on the security of human-generated patterns when the grid size is increased, as concluded in Aviv et al. [35]. I terms of how large the nodes are and how far apart they are on the screen, we have used the common Android lock patterns, as shown in Fig. 2(b).

3.2.3 Participants

Seven blindness and visually impaired participants with ages ranging from 21–23 took part in this study. They were recruited from Alnoor institution, Qassim, Saudi Arabia.

3.2.4 Uniqueness of the Vibration Feedback

The length of vibration has been studied in Saket et al. [36] in terms of designing an effective vibration-based notification interface for mobile phones. This study hence confirmed that the appropriate lengths for short and long signals are 200 ms and 600 ms, respectively. However, this result is only for helping users to prioritize the level of urgency of notifications. Thus, we use the results of this study as a basis for designing the vibration feedback in which the proposed approach is implemented. That is, we have designed two variants of vibration feedback: (1) feedback through vibration pulses which are counted by the user, and (2) feedback through vibration duration which has to be estimated by the user. These two variants require different abilities of the user and need to be reflected conceptually as well. Estimating timespans is properly much more difficult than counting individual pulses. Moreover, since we have used a grid size of 3 × 3, we need nine different vibration feedbacks to be assigned for each pattern.

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

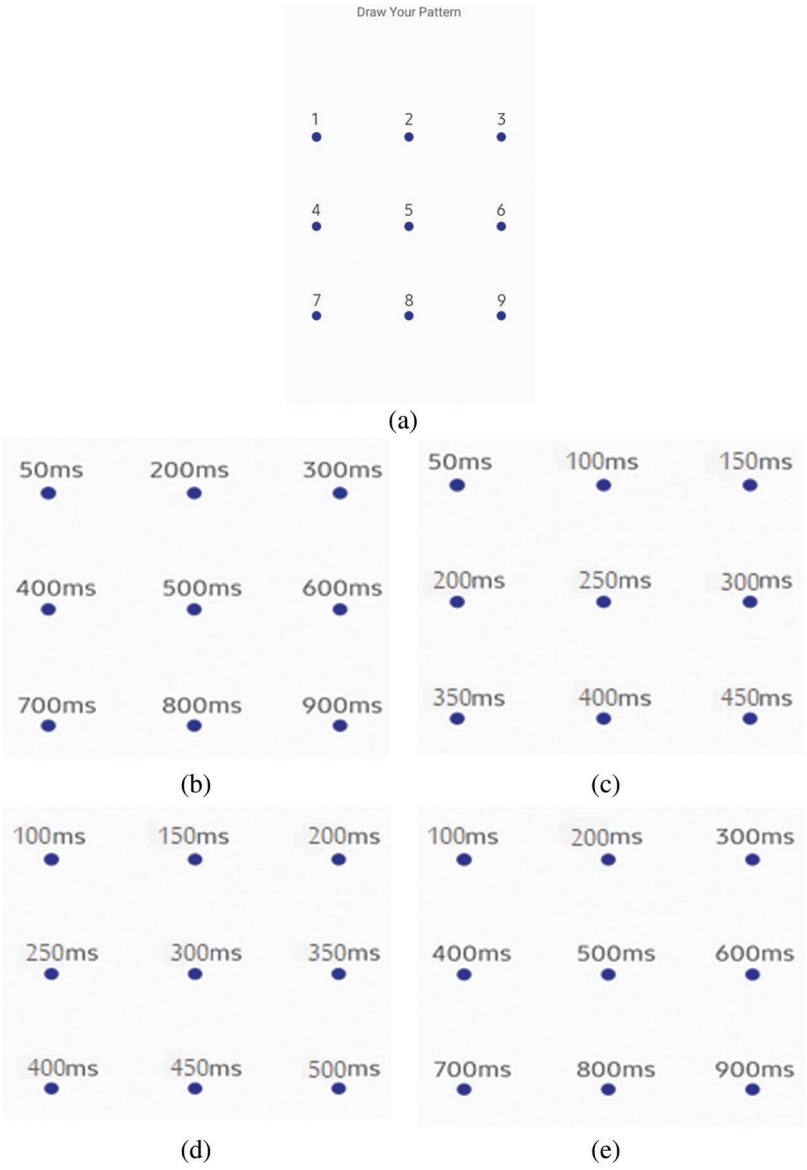

Figure 2: The proposed vibration length seniors: Vibration pulse (a) and Vibration duration (b–e)

First of all, for selecting a minimum understandable vibration feedback, users are asked to choose one of the following vibration feedback practically using the developed application as the most reasonable one in terms of sense of touch: 10, 20, 30, 40, and 50 milliseconds (ms). For this, these lengths are assigned to 1, 2, 3, 4, and 5 patterns, respectively. Therefore, the results of this showed that the users preferred 50 ms as a minimum understandable vibration feedback for each pattern. Besides, for the proposed vibration signal feedback, we have designed five vibration signal scenarios for each pattern, as shown in Fig. 2, one (i.e., Fig. 2(a)) as a vibration pulse, while the rest (i.e., Fig. 2(b–e)) as a vibration duration. Each scenario is described in the following.

In the pulses vibration, a touched pattern vibrates for a specific time based on its position (as shown in Fig. 2(a)). The length of each time is 50 ms. It is worth noting that this length is empirically estimated as explained previously. Although the pattern grid nodes are numbered from left to right from one to nine

(as shown in Fig. 2(a)), these numbers are used here for illustration purposes only, and do not appear on the developed application. For example, when node five is touched, it vibrates five times and each time it vibrates it lasts for 50 ms. Moreover, in order to reflect a selects password that is drawn in Fig. 3 using the pulses vibration scenario, the user should touch the nodes that produce the following vibration length: (50 ms × 1) + (50 ms × 4) + (50 ms × 7) + (50 ms × 5). Note that, "+" denotes to follow by.

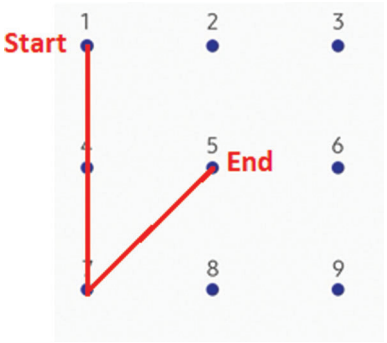

Figure 3: An example of a drawn pattern password

In the vibration duration, a specific vibration time is assigned to each node from 50 to 900 ms from one to nine respectively, as shown in Fig. 2(b–e)). For example, when node five in Fig. 2(b) is touched, it vibrates it lasts for 500 ms. Moreover, in order to reflect a select password that is drawn in Fig. 3 using the vibration duration shown in Fig. 2(b), the user should touch the nodes that produce the following vibration length: (50 ms) + (400 ms) + (700 ms) + (500 ms).

In order to select the appropriate scenario, the participants are asked to try all proposed vibration scenarios sequentially. In particular, once the participant is finished from each vibration scenario, the participant is asked to complete a short survey, which provided qualitative data on each participant's satisfaction in terms of the ability of estimating timespans of each pattern. This survey consisted of one item: "Have you correctly estimated the timespans of each pattern?" This item is ranked on a 5-point Likert scale: Strongly Agree, Agree, Neither Agree nor Disagree, Disagree and Strongly Disagree. The results of this, as shown in Fig. 4, showed that the normal vibration (Fig. 2(a)) and the vibration duration (Fig. 2(b)) were the most appropriate scenarios. Accordingly, these vibration scenarios will be utilized in Section 5.

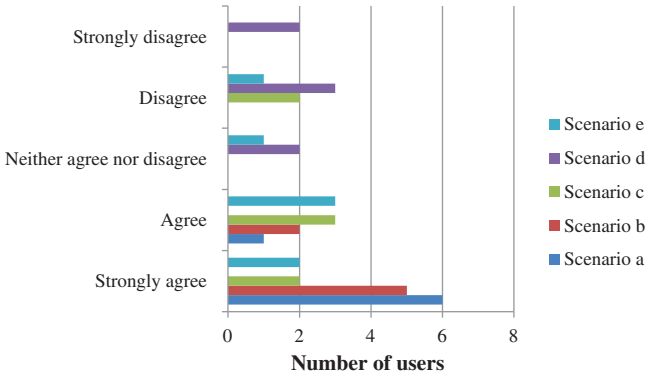

Figure 4: Results from qualitative measures for the proposed scenarios using the survey

4 Protection against Shoulder-Surfing Attack

The pattern authentication system developed by Google [37] is currently one of the most famous password authentication systems deployed. Despite the popularity of this system, it is vulnerable to shoulder-surfing attacks [3]. To provide a protection against this vulnerability, the camouflage patterns approach is used which has been developed in Alsuhibany [1]. In our paper, the camouflage pattern methodology is exploited by applying its concept to the proposed vibration-based authentication approach. The following section outlines the camouflage pattern methodology and how it is adapted in the proposed approach.

The camouflage pattern methodology is a number of nodes that can be selected randomly. In particular, it consists mainly two nodes: activation and deactivation. The activation node is preceded by a set of nodes that can be randomly chosen, while the deactivation node is followed by a set of nodes that can be randomly chosen. Finally, the password node is surrounded by these two nodes [1], as illustrated in Fig. 5. To set up these three nodes, they need to be chosen from the setting screen, as shown in Fig. 6, where the first node refers to the activation node, and the last node refers to the deactivation node [1]. It is remarkable to note that the password can include several nodes, which might make it more resist against the observation attack.

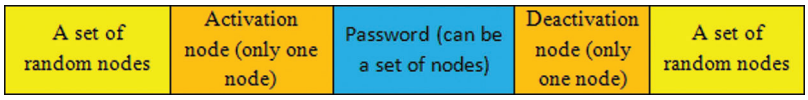

Figure 5: Creating a password using the proposed approach [1]

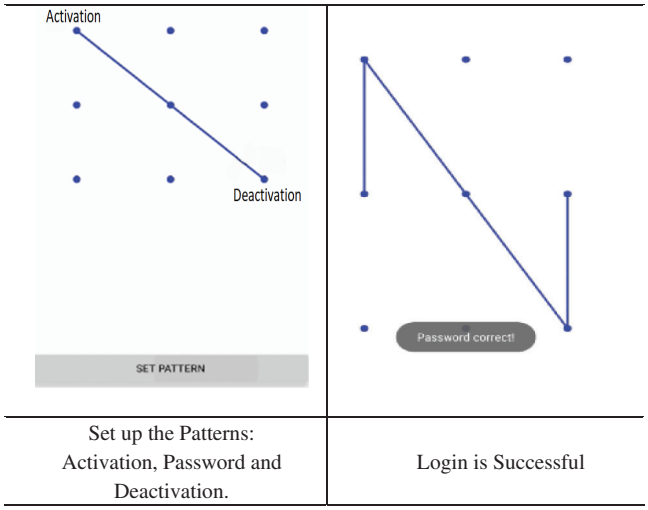

Figure 6: Setup the pattern and login using the camouflage pattern approach [1]

The implemented application of this methodology in the enrolment phase takes the first-chosen node as an activation node, the last-chosen node as a deactivation node and other nodes between these nodes are considered as a password. Furthermore, in the login phase as shown in Fig. 6, several patterns are allowed to be drawn, while the activation, password and deactivation nodes should be placed in a correct sequence in order to be authentication.

Thus, a complex *vibration* pattern is shown when several random camouflage vibration nodes are selected and linked them with each other. This may make capturing the developed vibration password

more difficult. For the usability aspect, it can also help users to remember it, as they only need to recall three vibration patterns: activation, password, and deactivation.

There are three techniques derived from the camouflage patterns methodology [1]: basic, non-repeated and alternation techniques. The results in Alsuhibany [1] showed that the non-repeated technique has higher ratings in both usability and security aspects. As a result, this technique is selected to be embedded in our proposed vibration-based authentication approach. It is interesting to note that the non-repeated technique works exactly like the basic approach explained here in this section with an additional feature that prevents the user from redrawing the same camouflage patterns twice in a row.

5 User Study and System Evaluation

This section explains the experimental study in which the proposed approach is evaluated in terms of the resistance to shoulder-surfing and usability. In the following sections, the experimental setup is described for each aspect as well as the procedure.

5.1 The Setup

This is to explain the participations, design type of the experiment and system.

5.1.1 Participants

Sixteen (16) blindness and visually impaired participants aged between 21–26 years old were recruited. They were recruited from Alnoor institution, Qassim, Saudi Arabia.

5.1.2 Design

A within-subject laboratory experiment is performed to compare aspects of shoulder-surfing resistance and usability between the selected vibration pulses and duration approaches. This study focuses on the effect of the design features of each approach related on the efficiency, effectiveness, and resistance to shoulder-surfing. Note, the main authentication *vibration* patterns are selected by users in order to make the experiment as realistic as possible.

5.1.3 System

An Android application is developed and implemented according to the description in Section 3 for the vibration pattern password approach. This application is then installed on two Android OS smart phones (Samsung Galaxy s6 edge and Lenovo).

5.2 The Procedure

This is to describe the way in which the experiment is carried out, including the instructions to the participants, the procedures for shoulder-surfing and usability and the collected data.

5.2.1 Shoulder-Surfing Experiment Procedure

The proposed approach's susceptibility to shoulder-surfing, with applying the camouflage pattern methodology, is assessed based on the success rate of the shoulder surfer, that is, how well the pressed password can be reproduced by an observer. To accomplish this, the proposed methodology in Shiraga et al. [38] is utilized based on a binary metric methodology in which the shoulder-surfing success is measured. In particular, if the participant entered the correct password within three attempts, then "1" is added; "0" otherwise.

Although the common approach is to have participants act as shoulder surfers (e.g., Higashikawa et al. [5]), in this case the experimenter acted as the shoulder surfer. The main reason for this is that the participants are visually impaired. Another reason is to reduce the inconsistency-bias that can be produced when using

two different persons to observe which can affect the results. It is important to note that the participants do not try to cover their devices or apply any defense techniques other than the one being tested. This is to make sure that the participant has no other method of protection. The experimenter was able to choose to stand either right behind the participants or behind their left shoulder. After the participant enters the password, the observer tries to login using the passwords, with a maximum of three attempts per observed password.

It is worthwhile noting that the participants were aware that the experimenter was engaged in shoulder-surfing.

5.2.2 Usability Experiment Procedure

The shoulder-surfing attack experiment is followed by the usability experiment. The usability of the proposed approaches is evaluated using qualitative and quantitative metrics. For the qualitative metrics, the data are collected from a short survey, which gives qualitative data about user satisfaction. For the quantitative metrics, the draw time required for login reflects the efficiency of the approach. Moreover, the entry time for each participant is recorded by the developed application. Finally, the login success rate for drawing a password reflects the effectiveness.

The participants are given a brief explanation of the study and details of the proposed approaches at the start of the experiment. This is followed by a short demonstration of how the system works, and a quick hands-on practice to guarantee that participants have some experience of using the developed prototype of the proposed approach before engaging in the actual tasks.

The participants are instructed for all approaches to complete the following tasks at the outset:

– To become familiar with the vibration pulses and duration approaches by creating their own main authentication *vibration* patterns.
– Then, to practice logging into the application.

To guarantee a sufficient amount of training, each participant is allowed to take roughly 20–25 minutes to complete these tasks. This time is determined during the pilot study. Following this, the participants are tutored to complete the following tasks: (1) to login using their own main authentication *vibration* patterns, and (2) to answer a short survey about the approach they have just used.

5.2.3 Collected Data

The shoulder-surfing success rates, draw time, login success rate for drawing and users' satisfaction are recorded.

6 Results

In the experiment, all participants completed the given tasks successfully. The shoulder-surfing success rates of the proposed approaches are presented followed by the usability results. This includes the efficiency, effectiveness, and satisfaction rates of the participants.

6.1 Shoulder-Surfing Results

As mentioned in Section 4, the experimenter acts as the shoulder-surfer throughout the study. Fig. 7 summarizes the total percentage of correctly guessed passwords for each type.

It is clear from these results that the vibration pulse approach is more secure than the vibration duration approach in terms of the resistance of a shoulder-surfing attack.

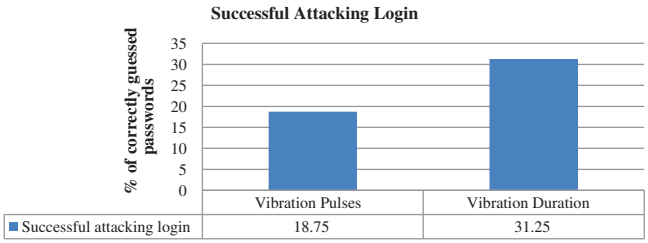

Figure 7: Summary of the total correctly guessed passwords for each type

6.2 Usability Results

The usability experiment is performed after the shoulder-surfing attack. This section presents the results of testing the entry time, login success rate, and satisfaction.

6.2.1 6.2.1 Entry Time (Efficiency)

The average time consumed on drawing the activation, password, and deactivation patterns for each type as shown in Fig. 8.

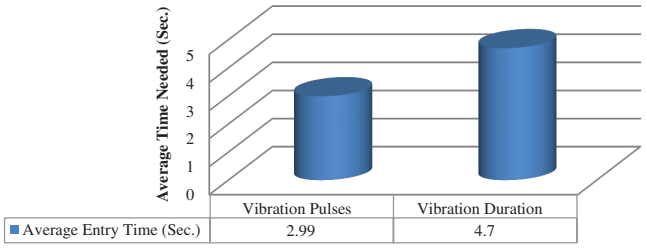

Figure 8: The average time consumed on drawing the activation, password, and deactivation pattern

6.2.2 Login Success Rate (Effectiveness)

This is reflected by the average of successful logins over all the attempts of one participant. Fig. 9 illustrates the average successful login rate for each type.

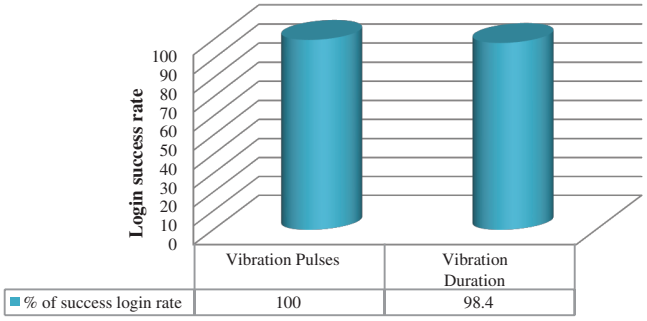

Figure 9: The average successful login rate for each type

6.2.3 Satisfaction

Tab. 1 illustrates the satisfaction results of each approach. Specifically, there are two questions should be answered by participants after carrying out all the given tasks. These questions are: Q1: *Are you willing to use*

these approaches on your devices? and Q2: *Which approach do you prefer in terms of authenticating your mobile device?*.

Table 1: The Satisfaction rates for of each vibration type

Yes/No	Q1	Vibration type	Q2
Yes	87.5%	Vibration Pulses	93.75%
No	12.5%	Vibration Duration	6.25%

7 Discussion

The findings indicate that the proposed vibration-based pattern password approach is helpful to the visually impaired for securing their devices. In particular, the vibration pulses type is the best in the usability testing with short password draw times, high levels of drawing accuracy and satisfaction. This type also has the best success rate in preventing shoulder-surfer attacks (18.75% compared to 31.25% for the duration vibration type).

Furthermore, the length of time for the vibration duration type is duplicated compared with the vibration pulses type (as explained in Section 3.1). For example, feedback for position 9:900 ms in the duration variant takes much longer than 9 × 50 ms = 450 ms in the pulse variant. This might be the reason for the negative implication for both the security and usability aspects. However, this implication might not apply to all users as some prefer this type (as shown in Tab. 1).

When comparing the results of the proposed approaches with the most relevant work, comparisons of the security and usability aspects along with some others are used (as shown in Tab. 2). Tab. 2 also shows that the vibration pulses approach is the fastest in terms of entry time. This approach is also more accurate than the other methods. Further, satisfaction levels are compared with those in other studies based on the first question in the survey (*Are you willing to use these approaches on your devices?*) and the vibration pulses approach is found to be more satisfactory than other approaches. Likewise, for the security aspect, the vibration pulses approach seems the best for resisting shoulder-surfing attacks.

Table 2: Comparison of security and usability aspects

Study	Usability			Security
	Entry time (s)	Login success rate	Satisfaction	Resistance to shoulder-surfing by eye
[14]	22.4	75%	NA	NA
[15]	37	74%	90%*	66.7%
Our	2.99**	100%**	87.5%**	81.25%**

*This percentage is derived from the study's results.

**Using vibration pulses type.

Dosono et al. [9] conclude that "the unique privacy and security needs of blind users remain largely unaddressed". Therefore, people with visual impairments will feel unable to securely preserve their digital information due to many factors like accessibility issues, the feedback provided [13] and the possibility of shoulder surfing for stealing their passwords [39]. Therefore, the proposed approach may contribute to filling this gap in the provision. A study in Faustino et al. [26] about understanding the authentication methods used on mobile devices by people with visual impairments found that pattern passwords were

one of not preferable accessible methods for people with visual impairments. However, the proposed approach demonstrates that pattern passwords with a vibration feature are satisfactory with a 100% effectiveness rate for people with visual impairments. By exploiting the camouflage patterns approach for this people, it can be helped to assure their digital security in the mobile context.

It is interesting to note that exploiting the camouflage patterns approach in this study allows the mobile to become unlocked using only the activation and the password nodes. It is also by using as many nodes as the user wants without the need to have a separate password. However, it can be complex at the early stages of use, and takes some getting used to. There might also be some cognitive load from the password drawer as users need to concentrate to which nodes are assigned to which roles. Although this might be a possible downside, it can also be a strong feature of the technique since every login is now unique. Furthermore, increasing the length and complexity of the password is one of the most important security factors, as concluded in Von Zezschwitz et al. [40], which can be found in the applied camouflage patterns approach.

It is worth mentioning that the security of the human generated patterns might be enhanced by utilizing the grid-size larger than 3 × 3. In contrast, a study in Aviv et al. [35] concludes that increasing the grid-size leads to a reduction in entering more complex patterns as the number of contact points becomes denser. Hence, our proposed approach provides a reasonable level of security as well as memorable password patterns while using only a 3 × 3 grid-size compared with other approaches.

The number of participants in this paper is quite low, which is a limitation to the work presented here. However, we consider this work as a proof of concept, showing that using a vibration-based authentication approach makes sense in some contexts. Clearly, a further work is required in order to understand which contexts are suitable and which are not.

Even though there are other user authentication methods available besides patterns (e.g., Fingerprint or Face recognition), there is no information regarding the preferable or considerable existing methods to be more secure and accessible for people with visual impairments. This, however, might be interesting to be investigated in the future.

8 Conclusion and Future Work

People with visual impairments are concerned about entering passwords into mobile devices when in public due to the risk of shoulder-surfing attacks, accessibility issues and the feedback provided. This paper proposes a vibration-based authentication approach that allows the visually impaired to use a pattern password. This provides two vibration feedbacks: pulses and duration. The security level of the proposed approach is enhanced using camouflage patterns. An experimental study is conducted to evaluate the proposal. The results of this experimental showed that the vibration pulses feedback is usable and practically resistant to shoulder-surfing attacks.

Our ongoing work is to investigate more vibration feedback like a combination of 3 different levels of pulse counts and vibration duration in order to create much faster entry speeds. Furthermore, we are going to develop a Voice-Based approach which can enable blind people to use Android unlock pattern with their voices. Although this approach works like the VoiceOver which pronounces the number of the nodes when pressed, the basic Camouflage Pattern Approach will be exploited. This makes it more fault tolerant where the user adds wrong nodes before and after the password, it also makes them more secure against shoulder surfing attacks.

Acknowledgement: Author would like to thank Qassim University for supporting this research.

Funding Statement: The author received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] 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. 11, no. 4, pp. 1645–1655, 2020.

[2] I. H. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The design and analysis of graphical passwords," in *Proc. of the 8th USENIX Security Sym.*, Washington DC, US, 1999.

[3] Y. Song, G. Cho, S. Oh, H. Kim and J. H. Huh, "On the effectiveness of pattern lock strength meters: measuring the strength of real world pattern locks," in *Proc. of the 33rd Annual ACM Conf. on Human Factors in Computing Systems*, Seoul, Republic of Korea, pp. 2343–2352, 2015.

[4] L. Bošnjak and B. Brumen, "Shoulder surfing experiments: A systematic literature review," *Computers & Security*, vol. 99, pp. 102023, 2020.

[5] S. Higashikawa, T. Kosugi, S. Kitajima and M. Mambo, "Shoulder-surfing resistant authentication using pass pattern of pattern lock," *IEICE Transactions on Information and Systems*, vol. 101, no. 1, pp. 45–52, 2018.

[6] S. Wiedenbeck, J. Waters, L. Sobrado and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proc. of the Working Conf. on Advanced Visual Interfaces*, Venezia, Italy, pp. 177–184, 2006.

[7] The Lighthouse National Survey on Vision Loss: Experience, Attitudes, and Knowledge of Middle-Aged and Older Americans: 1995. [Online]. Available: http://li129-107.members.linode.com/research/archived-studies/national-survey/. [Accessed: 01-03-2021].

[8] S. Azenkot, K. Rector, R. Ladner and J. Wobbrock, "PassChords: Secure multi-touch authentication for blind people," in *Proc. of the 14th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, Boulder Colorado, USA, pp. 159–166, 2012.

[9] B. Dosono, J. Hayes and Y. Wang, "I'm stuck!: A contextual inquiry of people with visual impairments in authentication," in *Proc. of the Eleventh Sym. On Usable Privacy and Security*, Ottawa, Canada, pp. 151–168, 2015.

[10] V. Balaji and K. S. Kuppusamy, "Towards accessible mobile pattern authentication for persons with visual impairments," in *2017 Int. Conf. on Computational Intelligence in Data Science (ICCIDS)*, Chennai, India, pp. 1–5, 2017.

[11] J. Lazar, B. Wentz and M. Winckler, "Information privacy and security as a human right for people with disabilities," in *Disability, Human Rights and Information Technology,* J. Lazar, M. Stein (eds.), Philadelphia: University of Pennsylvania Press, pp. 199–211, 2017.

[12] S. Maqsood, S. Chiasson and A. Girouard, "Bend passwords: Using gestures to authenticate on flexible devices," *Personal and Ubiquitous Computing*, vol. 20, no. 4, pp. 573–600, 2016.

[13] TalkBack, 2018. [Online]. Available: https://play.google.com/store/apps/details?id=com.google.android.marvin.talkback&hl=en. [Accessed: 07-02-2021].

[14] iOS Accessibility, 2014. [Online]. Available: http://www.cnib.ca/en/living/how-to-videos/tools-and-tech/Pages/iOSaccessibility.aspx. [Accessed: 07-02-2021].

[15] S. Azenkot and N. B. Lee, "Exploring the use of speech input by blind people on mobile devices," in *Proc. of the 15th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, New York, USA, pp. 1–8, 2016.

[16] M. Alnfiai and S. Sampalli, "An evaluation of SingleTapBraille keyboard: A text entry method that utilizes Braille patterns on touchscreen devices," in *Proc. of the 18th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, Reno Nevada, USA, pp. 161–169, 2016.

[17] J. Oliveira, T. Guerreiro, H. Nicolau, J. Jorge and D. Gonçalves, "BrailleType: Unleashing Braille over touch screen mobile phones," in *IFIP Conf. on Human-Computer Interaction*, Lisbon, Portugal, pp. 100–107, 2011.

[18] D. B. Faustino and A. Girouard, "Bend passwords on Bendypass: A user authentication method for people with vision impairment," in *Proc. of the 20th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, pp. 435–437, 2018.

[19] D. B. Faustino, "Bend passwords for people with vision impairment," PhD dissertation. Carleton University, Ottawa, 2018.

[20] J. Hayes, S. Kaushik, C. E. Price and Y. Wang, "Cooperative privacy and security: Learning from people with visual impairments and their allies," in *Fifteenth Sym. on Usable Privacy and Security (SOUPS)*, Santa Clara, USA, pp. 1–20, 2019.

[21] M. M. Haque, S. Zawoad and R. Hasan, "Secure techniques and methods for authenticating visually impaired mobile phone users," in *2013 IEEE Int. Conf. on Technologies for Homeland Security (HST)*, Waltham, MA, USA, pp. 735–740, 2013.

[22] R. Wang, C. Yu, X. D. Yang, W. He and Y. Shi, "EarTouch: Facilitating smartphone use for visually impaired people in mobile and public scenarios," in *Proc. of the 2019 CHI Conf. on Human Factors in Computing Systems*, Glasgow, UK, pp. 1–13, 2019.

[23] M. Alnfiai and S. Sampalli, "BraillePassword: Accessible web authentication technique on touchscreen devices," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 6, pp. 2375–2391, 2019.

[24] T. Ahmed, "Towards the design of wearable assistive technologies to address the privacy and security concerns of people with visual impairments," PhD dissertation. Indiana University, Bloomington, 2019.

[25] N. M. Barbosa, J. Hayes and Y. Wang, "UniPass: Design and evaluation of a smart device-based password manager for visually impaired users," in *UbiComp*, Heidelberg, Germany, pp. 49–60, 2016.

[26] D. B. Faustino and A. Girouard, "Understanding authentication method use on mobile devices by people with vision impairment," in *Proc. of the 20th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, Galway, Ireland, pp. 217–228, 2018.

[27] W. Grussenmeyer and E. Folmer, "Accessible touchscreen technology for people with visual impairments: A survey," *ACM Transactions on Accessible Computing (TACCESS)*, vol. 9, no. 2, pp. 1–31, 2017.

[28] C. Jayant, C. Acuario, W. Johnson, J. Hollier and R. Ladner, "V-Braille: Haptic Braille perception using a touch-screen and vibration on mobile phones," in *Proc. of the 12th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, Orlando, Florida, USA, pp. 295–296, 2010.

[29] L. R. Milne, C. L. Bennett, R. E. Ladner and S. Azenkot, "BraillePlay: Educational smartphone games for blind children," in *Proc. of the 16th Int. ACM SIGACCESS Conf. on Computers & Accessibility*, Rochester, New York, USA, pp. 137–144, 2014.

[30] Y. L. Ho, B. Bendrissou, A. Azman and S. H. Lau, "BlindLogin: A graphical authentication system with support for blind and visually impaired users on smartphones," *American Journal of Applied Sciences*, vol. 14, pp. 551–559, 2017.

[31] F. Schaub, M. Walch, B. Könings and M. Weber, "Exploring the design space of graphical passwords on smartphones," in *Proc. of the Ninth Sym. on Usable Privacy and security*, New York, NY, USA, pp. 1–14, 2013.

[32] J. L. Tennison, P. M. Uesbeck, N. A. Giudice, A. Stefik, D. W. Smith *et al.,* "Establishing vibration-based tactile line profiles for use in multimodal graphics," *ACM Transactions on Applied Perception (TAP)*, vol. 17, no. 2, pp. 1–14, 2020.

[33] J. Yim, R. Myung and B. Lee, "The mobile phone's optimal vibration frequency in mobile environments," in *Int. Conf. on Usability and Internationalization*, Beijing, China, pp. 646–652, 2007.

[34] K. Stopar, "Device for visual kinesthetic navigation of the blind and visually impaired," in *2020 IEEE 20th Mediterranean Electrotechnical Conf. (MELECON)*, Palermo, Italy, pp. 646–651, 2020.

[35] A. J. Aviv, D. Budzitowski and R. Kuber, "Is bigger better? Comparing User-Generated Passwords on 3 × 3 *vs.* 4 × 4 Grid Sizes for Android's Pattern Unlock," in *Proc. of the 31st Annual Computer Security Applications Conf.*, Los Angeles, CA, USA, pp. 301–310, 2015.

[36] B. Saket, C. Prasojo, Y. Huang and S. Zhao, "Designing an effective vibration-based notification interface for mobile phones," in *Proc. of the 2013 Conf. on Computer Supported Cooperative Work*, San Antonio, Texas, USA, pp. 149–1504, 2013.

[37] R. Biddle, S. Chiasson and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, pp. 1–41, 2012.

[38] S. Shiraga, Y. Kinoshita and K. Go, "Designing smartphone feedback based on vibration impression," in *Proc. of the 2016 CHI Conf. Extended Abstracts on Human Factors in Computing Systems*, San Jose, California, USA, pp. 3190–3196, 2016.

[39] H. Ye, M. Malu, U. Oh and L. Findlater, "Current and future mobile and wearable device use by people with visual impairments," in *Proc. of the 32nd Annual ACM Conf. on Human Factors in Computing Systems—CHI '14*, Toronto, Canada, pp. 3123–3132, 2014.

[40] E. Von Zezschwitz, A. De Luca, P. Janssen and H. Hussmann, "Easy to draw, but hard to trace? On the observability of grid-based (un) lock patterns," in *Proc. of the 33rd Annual ACM Conf. on Human Factors in Computing Systems*, Seoul, Republic of Korea, pp. 2339–2342, 2015.