symmetry

MDPI

Article

An Efficient Login Authentication System against Multiple Attacks in Mobile Devices

Yang Li [1,*], Xinyu Yun [1], Liming Fang [1,*] and Chunpeng Ge [1,2,3]

[1] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, NO. 29 Yudao Street, Nanjing 210016, China; yunxinyu@nuaa.edu.cn (X.Y.); gecp@nuaa.edu.cn (C.G.)
[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
[3] Science and Technology on Parallel and Distributed Processing Laboratory (PDL), Changsha 410003, China
* Correspondence: lyang0314@nuaa.edu.cn (Y.L.); fangliming@nuaa.edu.cn (L.F.); Tel.: +86-159-2999-0112 (Y.L.); Tel.: +86-186-2685-8383 (L.F.)

Abstract: Access management of IoT devices is extremely important, and a secure login authentication scheme can effectively protect users' privacy. However, traditional authentication schemes are threatened by shoulder-surfing attacks, and biometric-based schemes, such as fingerprint recognition and face recognition, that are commonly used today can also be cracked. Researchers have proposed some schemes for current attacks, but they are limited by usability. For example, the login authentication process requires additional device support. This method solves the problem of attacks, but it is unusable, which limits its application. At present, most authentication schemes for the Internet of Things and mobile platforms either focus on security, thus ignoring availability, or have excellent convenience but insufficient security. This is a symmetry problem worth exploring. Therefore, users need a new type of login authentication scheme that can balance security and usability to protect users' private data or maintain device security. In this paper, we propose a login authentication scheme named PinWheel, which combines a textual password, a graphical password, and biometrics to prevent both shoulder-surfing attacks and smudge attacks and solves the current schemes' lack of usability. We implemented PinWheel and evaluated it from the perspective of security and usability. The experiments required 262 days, and 573 subjects participated in our investigation. The evaluation results show that PinWheel can at least effectively resist both mainstream attacks and is superior to most existing schemes in terms of usability.

Keywords: login authentication; shoulder-surfing attack; privacy security

check for updates

Citation: Li, Y.; Yun, X.; Fang, L.; Ge, C. An Efficient Login Authentication System against Multiple Attacks in Mobile Devices. *Symmetry* **2021**, *13*, 125. https://doi.org/doi:10.3390/sym13010125

Received: 12 December 2020
Accepted: 6 January 2021
Published: 13 January 2021

1. Introduction

With the rapid development of Internet technology, various smart devices are connecting through the Internet and using the convenience of the Internet to disseminate information to realize various functions such as automatic reporting of data, remote accessing, and remote control management.

Authentication security on IoT devices: Many IoT devices are unguarded most of the time, requiring users to remotely manage devices over the network, or the devices share collected information with specific users. Most of this information contains privacy attributes, so access management and authentication are very important. Researchers have put much effort into the research of authentication schemes to prevent these schemes from being cracked by different attacks. However, new attacks are continuously proposed and diverse. The emergence of shoulder-surfing attacks and smudge attacks makes traditionally widely used login authentication schemes increasingly vulnerable, thus threatening the security of users' private data [1]. A survey conducted by researchers specifically for shoulder-surfing attacks showed that 35% of participants were worried that someone might observe them and steal their certificates when the smart device is unlocked [2,3]. The study also notes that when shoulder-surfing attacks are carried out in private, the potential attackers are usually malicious insiders, such as colleagues or family members. In addition, there are also cases in which password leakage caused by shoulder-surfing attacks result in substantial property loss [4].

Serious problems with traditional schemes: In past login authentication schemes, the login authentication scheme using a PIN has been widely used because of its convenient operation and good resistance to brute force attack [5]. However, simple textual passwords are less secure, and powerful textual passwords provide users with a memory burden that cannot be ignored [6,7] and often lead to password reuse problems. Researchers have proposed graphical login authentication schemes for this problem [8,9]. Although these passwords are easy to remember, they are vulnerable to shoulder-surfing attacks [10,11]. In popular graphical login authentication schemes, the trajectory left by the user on the screen is traceable and easy to analyze, so it is also unable to resist smudge attacks. Some researchers have proposed some schemes for these attacks, but they have poor portability (for example, users who need additional headphones or other devices when logging in [12]) and the use of scene-limited weaknesses [13]. Since then, some researchers have proposed biometric-based authentication schemes, such as fingerprint recognition and face recognition, but recently reported that they have been cracked, which means that they cannot effectively protect users' privacy. People need a new login authentication scheme to simultaneously defend against various attacks and have good usability.

Designing to address these challenges: To solve a series of problems faced by traditional authentication schemes, this paper designs a login authentication scheme based on graphical passwords and biometrics named PinWheel. The scheme transmits the random challenge value required for each login according to the fixed bead selected by the user at the time of registration, and the user must correspondingly enter the challenge value transmitted by the system into the correct area for authentication. This scheme combines a location password with a textual password to enable the device to prevent a malicious attacker from performing a shoulder-surfing attack, smudge attack, or video analysis attack to obtain a user password. In addition, PinWheel also adds an optional user feature-based authentication mechanism that allows only trusted administrators to login to secure devices and protects the security of devices and privacy data.

In this work, we designed an attack experiment to test the security performance of PinWheel by repeating several attacks. The result was positive. We also designed and implemented a long-term user study for PinWheel. We mainly collected relevant data from the subjects, such as the time spent on authentication and the long-term memory of passwords. The direct source of these data was a beta version of PinWheel that users installed on their mobile devices. In addition, we designed a questionnaire to assist information collection in the latter period of the experiment. The results proved that PinWheel has good usability.

In summary, our paper makes the following contributions:

1. We propose a secure and reliable login authentication scheme named PinWheel for IoT devices or mobile terminals that control IoT devices. PinWheel can resist shoulder-surfing attacks, smudge attacks, and video analysis attacks, and its security is greatly improved compared to traditional graphical login authentication schemes.
2. We implemented PinWheel (in Android and iOS) and reproduced several different attacks. We designed security experiments for each attack to verify the security of PinWheel. The experimental results showed that PinWheel has good resistance to the above three attacks. The success rate of the shoulder-surfing attack and smudge attack was zero.
3. We collected a large dataset of PinWheel usage behaviors from 573 subjects and a multitouch feature dataset to analyze user habits and changes in behavioral features over time.
4. We designed a user investigation for PinWheel, studied the actual performance of PinWheel through usability experiments, and combined the investigation to explore

the subjects' acceptance of PinWheel, their propensity to use, and their perception of authentication security.

The rest of the paper is organized as follows. Section 2 introduces the relevant investigation analysis and defense schemes. Then, our PinWheel scheme is detailed in Section 3. In Section 4, to verify the security of PinWheel, we simulate the attack of PinWheel. In Section 5, to obtain the users' true reflection, we evaluate the PinWheel through the user study from different points of view, such as registration and login time. Finally, we discuss PinWheel and conclude the paper in Sections 7 and 8.

2. Related Work

2.1. Analysis and Investigation

Por et al. [10], in the study of shoulder-surfing attack, first used the directed graph replacing rules in PlayFair cipher to experiment. PlayFair cipher is a modern cryptography method, which belongs to the intersection of mathematics and computer science, but this proved to be insufficient to prevent shoulder-surfing attack. In addition, the authors also used directed graph replacing rules and output feedback methods to determine the pass-image. Through users' research, the authors proved that this improved method was robust to direct observation and video recording of shoulder-surfing attack.

Saad et al. [14] reported a user study showing that vibrotactile feedback is superior to other feedback modes. Although protecting the authentication process of mobile devices from shoulder-surfing attack has received considerable attention (for example, through various forms of biometric authentication [15]), the interactive process is still vulnerable to such attacks. In this paper, the authors were committed to protecting users from shoulder-surfing attack throughout the interaction. The authors believed that one of the main challenges in preventing shoulder-surfing attack is to identify the attacker. This is a challenge when the attacker is in a dead zone, either behind or on the side of the user. To address this challenge, the authors proposed DSSytem, a system that can detect shoulder surfers and issues attack notifications to users. It uses the front camera of the mobile device to detect shoulder surfers peeking from behind the user and uses four different feedback methods to notify the user, namely vibration-tactile feedback, front LED flashing, icon screen overlay, and live video streaming. The authors elaborated on the user-centric design process of DSSytem and compared different feedback methods.

2.2. Defense Scheme

Wu et al. [16] proposed a new secure shoulder-surfing defense (SSP) graphical password authentication system. They used the convex-hull graphical algorithm to determine the authentication area, but changed the input password method. This can prevent attackers from observing the clicked position with the mouse directly to resist shoulder-surfing attack and complicate the selection of positions by adding dynamically moving colored balls on the screen. When a ball corresponding to the password enters the authentication area, the user only needs to press the space bar to confirm. Users must remember the password pattern and its color when registering and then perform the correct steps during the authentication phase. However, this solution is difficult to implement on smartphones and other devices because the screen is too small.

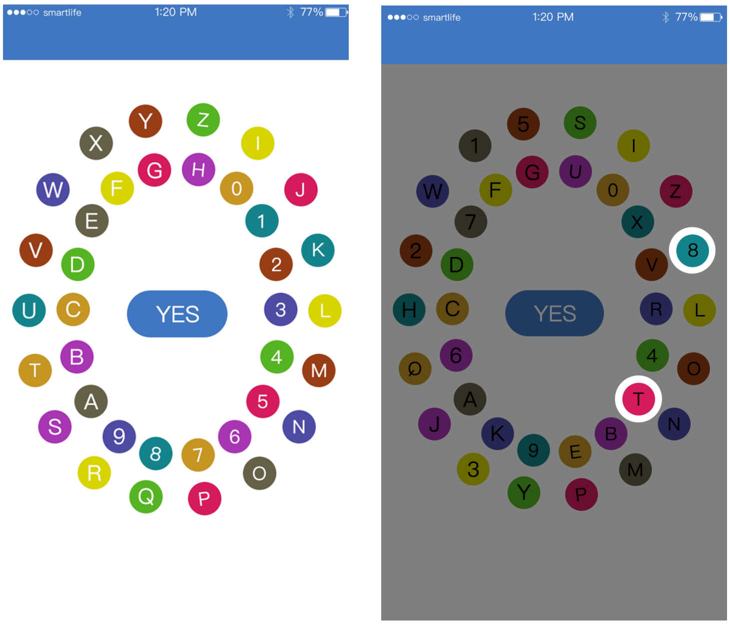
Zhou et al. [17] designed a polynomial-based Google maps graphical password (P-GMGP) system to combat shoulder-surfing attack. This system not only effectively resists shoulder-surfing attack, but also greatly reduces the time complexity of authentication. In a cloud environment, users usually need to access different types of services or data resources from multiple servers, and the original P-GMGP system can be easily extended, allowing users to authenticate through M servers simultaneously. Because the extended P-GMGP system allows users to be authenticated by M servers at the same time, it is very suitable for multi-server environments. In the P-GMGP system and the extended P-GMGP system, since the user does not need to directly click the password point to pass the authentication, both can effectively resist shoulder-surfing attack. However, this solution cannot resist a powerful attack capable of video analysis attack.

Chen and Zhu proposed a new method MapPass [18], which can use the attacker's cognitive dead zone, thus resisting shoulder-surfing attack. This method uses a combination of multiple password numbers and letters to display on the same screen and transmits implicit information like the user to confuse the attacker. However, such a scheme may be effective for an attacker who observes the login process for the first time. For an attacker who can obtain the authentication process multiple times, such a design is easy to crack.

3. Prototype Design and Implementation

3.1. Overview of PinWheel

This paper proposes a login authentication scheme named PinWheel, which does not require other media to spread the challenge value. The user only needs to perform some simple operations on an IoT device or mobile terminal that controls IoT devices and can effectively prevent shoulder-surfing attacks. The login is divided into two different phases. For the user, there is a first password and a second password, which respectively correspond to two different login authentication phases. First, we create a user interface that can sense gestures on the screen. The first phase of login authentication is shown in Figure 1a.


●●●○○ smartlife
1:20 PM
77%
Y Z X I G H W F 0 J E 1 V D 2 K U C
YES
3 L T B 4 M A 5 S 9 6 N 8 7 R O Q P
●●●○○ smartlife
1:20 PM
77%
5 S 1 I G U W F 0 Z 7 X 2 D V 8 H C
YES
R L Q 6 4 O A T J N K B 9 E 3 M Y P

(**a**) Initial interface.

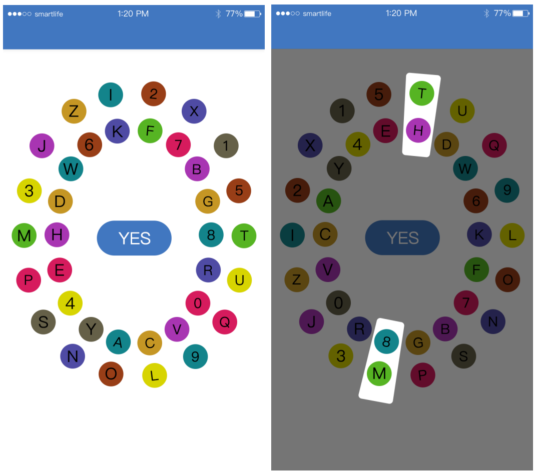
(**b**) The system implicitly passes "8, T" as the login indicator to the user.

Figure 1. The first phase of login authentication.

The PinWheel interface: The password wheel in Figure 1a consists of two oval digital wheels divided into an inner wheel and an outer wheel. The inner wheel and outer wheel are composed of 18 beads with numbers and letters, respectively, and have different colors. The distribution of bead colors is different at different login phases, which is described in detail later. The bead for each color is repeated four times. Each bead corresponds to the numbers 0–9 and the letters a–z. According to the different gesture operations of the user, the inner and outer password wheels can be rotated independently of each other, and the bead and the PIN contained therein can be rotated to the next location. The process of rotating each bead one turn on the wheel goes through 18 locations.

Registration Phase 1 and Login Phase 1: When the user sets the password, he or she needs to choose two passwords, corresponding to the two phases of the login authentication process. In the first phase of the password registration process, the user can arbitrarily set the distribution of the beads' colors according to his or her preferences. After the setting, the arrangement rules of the various colors of beads are fixed (only in the first phase) and are followed by the first phase of the login authentication process. After the setup is complete, the user is asked to select the bead in the two locations in order, i.e., select the bead in a certain location twice. In addition to the location and color of the bead, the order of selection also needs to be remembered. We will record the location information and the selection order of this phase as Location 1. This is the password for the first phase of the user login authentication process. It should be noted that in the password selection and registration at this phase, the screen does not contain numbers and letters, and the user does not have to focus on this. In the first phase of the login authentication process, according to the user's previous selection of the beads' arrangement rules (including the location and colors of the beads), the numbers 0–9 and the letters a–z are randomly filled into each bead. The user can obtain the two digit challenge value transmitted by the system to the user in order by the selected beads' location information when registering, and the content of the challenge value is derived from the PIN in the beads selected by the user. During this login authentication phase, the password wheel is fixed and cannot be rotated. The two digit challenge value obtained by the user is used to pass to the next login authentication phase. The user in Figure 1b obtains the challenge value "8, *T*" transmitted by the system for the user during the login authentication process according to the location and selection order of the beads selected by the user.

Registration Phase 2 and Login Phase 2: During the second phase of the password registration process, the user is asked to select two different "areas" in order, but this time, only the area information and the selection order need to be remembered and the user does not need to address any information related to the bead (however, the two digit challenge value obtained from the bead in the previous login phase needs to be remembered). The definition of the "area" is shown in Figure 2a. On the entire password wheel, we divide every two beads into groups, which are divided into 18 different areas. One area contains an inner wheel bead and an outer wheel bead. We record the area information and the order of the selection obtained in this phase as Location 2. In the second phase of login authentication, the color of the bead and its PIN are randomly distributed in each location of the password wheel. In other words, each time the second phase of login authentication is entered, the arrangement of the bead and PIN is random and refreshed and not known in advance; this is not related to the arrangement rules of the first phase user-defined settings, as shown in Figure 2b. In this login authentication phase, the user can rotate the password wheel. At this time, the user needs to rotate the bead corresponding to the two digit challenge value just obtained from the first phase to the area of Location 2 in order. The two digit challenge value and the location of the two areas of Location 2 correspond in order. The challenge value in the previous order is rotated to the first area, and the subsequent challenge value is rotated to the second area. In this way, although the location of the letters and numbers is randomly generated and may be generated in the inner wheel, it may be generated on the outer wheel, but the user only needs to rotate the challenge value to the corresponding area in order, which may correspond to the inner wheel bead or the outer wheel bead. Whether it is the inner wheel or the outer wheel, for a certain area, there is only one specific corresponding bead. The user must complete the unlocking by sequentially matching the challenge values to the correct area. The overview of PinWheel is shown in Figure 3. It should be read from top to bottom, with registration steps at the top and authentication steps at the bottom. Starting from the top step of Figure 3, each step is issued by the system or user, and the overall interaction logic is asynchronous.



(**a**) The initial state of the second stage.

(**b**) The user correctly corresponds the login indicator to the area.

Figure 2. The second phase of login authentication.

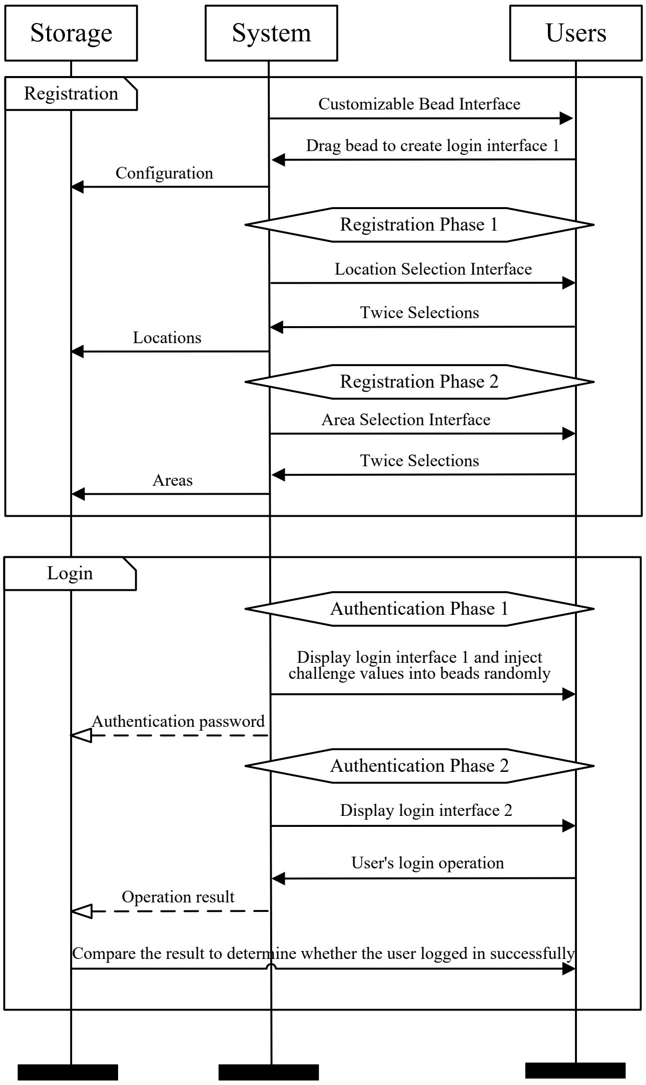


Figure 3. Flowchart of PinWheel.

3.2. Insights of the Design

In the first phase of the user login, the password wheel is completely static, and the location and number arrangement of different colorful beads cannot be changed by swiping the screen. It is only for the user to implicitly obtain the challenge value used in the second phase. The color design of the bead was added to the PinWheel interface because the user can easily find the corresponding two key beads when obtaining the two digit challenge value. The color information does not act as the user's login password. In addition, the color of the beads can effectively prevent shoulder-surfing attacks. The user login interface has 36 beads carrying information at the same time, and both carry color information, which makes it difficult to obtain the login information completely for the naked human eye and an ordinary camera. In the experiment, we confirmed that this method works very well.

For the setting of the "region" concept, it is also possible to increase the difficulty of the attacker analysis. Because in the second phase of login, the challenge value is refreshed in the inner wheel or outer wheel, there are four variants in the corresponding locations of the two digit challenge values: "the inner wheel + the inner wheel", "the inner wheel + the outer wheel", "the outer wheel + the inner wheel", and "the outer wheel + the outer wheel". This kind of location randomly changes, and to a certain extent, it also increases the difficulty of the password mechanism being cracked.

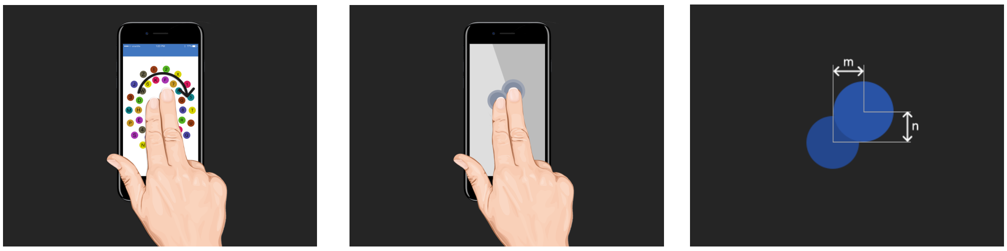
The user only needs to remember the login to the two locations: "Location 1" in the first phase in order and the login to the two regions "Location 2" in the second phase. The experiments in Section 5.4 show that this does not create a large memory burden for users.

3.3. Extension of PinWheel

Considering the user's needs for different security, we also added some extension options for PinWheel. In the original PinWheel, to balance the security and convenience considerations, we expect users to use two bead locations as their passwords, but we also allow users to expand it to three. Correspondingly, the user can also select three locations. During the login authentication process, according to the logic of the original PinWheel, the challenge values transmitted by the three bead locations selected by the user are correctly mapped to the three locations, which was allowed when the PinWheel was designed. This would be reflected in the registration process. Users could choose whether to add PinWheel's expansion scheme during the original registration, which means that the complexity of user passwords would increase and security would be more guaranteed. However, we think this has an impact on the login time, and the difficulty of remembering the password also increases. Considering most of the different views on the expansion scheme, we define this expansion and the biometric module to be introduced in Section 3.4 as the part that the user can choose whether to use. In the user study in Section 5, we also elaborate on the login time of the extension scheme and the subjects' views on the significance of the extension's application.

3.4. Biometric Authentication Module

To address more secure scenarios and a small number of powerful attackers (for example, multiple video analysis attacks), we also added an optional biometric module to PinWheel. Users can choose whether to use the module according to their security needs. The main working principle of this module is as follows: in the second phase of user login, the user is required to use two fingers to swipe the screen to control the rotation of the inner and outer wheels, as shown in Figure 4a–c. The user's feature value is represented by two length values, which are the lateral distance and the longitudinal distance between the touch points of the two fingers. These two values also differ depending on the features of the user's finger. By observing the feature values, whether the current operator is a registered user can be determined. The identification method is similar to fingerprint identification, which is widely used currently. We extract the local features from the user's sliding track, including: 1. the horizontal distance and vertical distance of two starting points. 2. the horizontal distance and vertical distance of the highest points. 3. the horizontal distance and vertical distance of two termination points. After obtaining the complete track, we first extract feature points and then do feature matching. This improves the security of the login, even if the attacker has completely obtained the user's password, but if the user's finger features cannot be accurately simulated, the authentication cannot be successfully completed. We tested 85 users in subsequent experiments, and the experimental results proved this. Among the 85 participants, seventy-six can successfully pass the test for the first time, and six can pass the test for the second time. As for the remaining three failed users, we think that the reason for their failure is related to the wrong information collection during registration.



(**a**)User can operate with two fingers. (**b**)Feature collection. (**c**)Integrate and calculate features.

Figure 4. The description of the biometric authentication module.

Because authentication exists in the process of the user sweeping the screen to unlock, it is not necessary to spend special time specifically performing feature recognition, and a relatively lightweight calculation can be used to achieve a significant recognition effect. The design of this module is based on the following design goals:

- Easy to operate, avoiding any user difficulty in use.
- High recognition efficiency and recognition accuracy with lightweight calculations.
- Avoid user characteristics changing with high frequency, and the user can use it for a long time without resetting.

3.5. Introduction of the Module

3.5.1. Indicator Generator Module

The indicator generator has two main dimensions, color and number. The module randomly generates nine colors into 36 beads; the same color has four beads; and 0–9, a–z are randomly arranged into 36 beads. It is worth mentioning that in the first phase of login, the distribution of the beads' colors is fixed, set by the user registration phase, and the color of the second phase beads is randomly generated each time the user logs in. The numbers and letters contained in the beads in the login phase are randomly generated, which applies to the first phase and the second phase of the login.

3.5.2. Communication Module

This module ensures the transfer of information between the client and the server. The entire communication process is protected by SSL to ensure data transmission security.

3.5.3. Verification Module

This module is used to verify that the user password is entered correctly. It is used to detect the correspondence between the two digit challenge value and the authentication area, and unlocking can only be completed if the user enters correctly twice.

3.5.4. Gesture Sensing Module

The module can sense the user's operation gesture on the touchable screen, and the user slides his or her fingers to the left or right in different areas to operate the outer wheel and the inner ring to the left or the right to move the bead.

3.5.5. Feature Recognition Module

The module senses the user's finger features, that is the horizontal distance and the vertical distance of the points when the two fingers perform the sliding operation on the screen.

3.5.6. Database Module

The database can store login information for multiple users, including the account name and password settings.

4. Attack Experiment

4.1. Experimental Setup

Experimental purpose: The purpose is verify the security of PinWheel by simulating an attack on PinWheel. Experimental design: From the perspective of the attacker, we simulate shoulder-surfing attacks, smudge attacks, and video analysis attacks on PinWheel. Experiment preparation: A total of 140 subjects participated in these attack experiments. As with most related works [19,20], the subjects were grouped from the perspective of attackers and ordinary users and participated in different attack experiments. Before the beginning of these experiments, we trained the subjects to ensure that they understood the use of PinWheel and could operate PinWheel proficiently. For the group of subjects acting as ordinary users, we provided a safe and independent environment for registering PinWheel and ensuring transmission security between the client and the server. For the group of subjects acting as attackers, we hid the password information of the ordinary users and elaborated on the purpose and method of the attack.

4.2. Experimental Implementation

When implementing attack experiments, we verified the security of PinWheel from the perspectives of shoulder-surfing attacks, smudge attacks, and video analysis attacks.

4.2.1. Shoulder-Surfing Attack

Generally, there are two types of shoulder-surfing attacks in public: naked-eye attacks and camera attacks. In the former, the attacker stands behind an ordinary user's shoulder and observes with the naked eye. The difference in attack distance and angle can produce different results. In this experiment, we uniformly ordered the attacker to stand 0.5 m behind the shoulders of the ordinary users. The latter generally uses a camera to record the phone's screen, and the attacker performs attacks by observing the video recorded by the camera. In this experiment, the camera was located behind the ordinary users to ensure that the phone's screen and user's operation can be fully captured.

In this experiment, a total of 60 subjects participated, and the experiment took 6 days. We divided the subjects into 20 groups of two attackers and one ordinary user. One of the attackers carried out a naked-eye attack, and the other attacker carried out a camera attack. Ordinary users performed 1, 2, 3, and 5 normal login authentication operations according to the user manual.

4.2.2. Smudge Attack

Smudge attack refers to a hacker performing an attack based on the smudges left by ordinary users when operating the mobile phone's screen. In this experiment, a total of 40 subjects participated, and the experiment took 4 days. We divided the subjects into 20 groups of one attacker and one ordinary user in each group. Ordinary users performed 1, 2, 3, and 5 normal login authentication operations according to the user manual, and for each operation, we took photos of the smudges left on the screen and collected them; then, the attacker analyzed the smudges based on the photos.

4.2.3. Video Analysis Attack

Video analysis attack refers to an attacker installing malicious screen recording software inside the mobile phone to record the user's login authentication process and performing the attack by observing the recorded video. Unlike shoulder-surfing attacks, video analysis attacks can obtain more detailed screen information for analysis, and the attacker can repeatedly observe and infer.

In this experiment, a total of 40 subjects participated, and the experiment took 4 days. We divided the subjects into 20 groups of one attacker and one ordinary user in each group. Ordinary users performed 1, 2, 3, and 5 normal login authentication operations according to the user manual, and each operation process was recorded by the screen recording software. The attacker analyzed the login according to the recording process.

4.3. Experimental Results and Analysis

In these attack experiments, we completed $2 \times 20 \times 4 + 20 \times 4 + 20 \times 4 = 320$ attacks, including 160 shoulder-surfing attacks, 80 smudge attacks, and 80 video analysis attacks, and the total attack success rate was not very high, as shown in Table 1.

Table 1. Experimental results.

Attack	**Shoulder-Surfing**		**Smudge**	**Video Analysis**
Attack Type	**Naked-Eye**	**Camera**		
1	0	0	0	0
2	0	0	0	0
3	0	0	0	1
5	0	0	0	2

4.3.1. Shoulder-Surfing Attack

The experimental results of the shoulder-surfing attacks are shown in Table 2. The naked-eye attack and the camera attack were performed 80 times each, with zero successes. According to the subjects' feedback acting as attackers, the inherent characteristics of the PinWheel interface made it difficult for shoulder-surfing attacks to recognize the password. In addition, the user's fast operation speed made them unable to capture effective screen information, which made the attack more difficult.

Table 2. Experimental results of shoulder-surfing attack.

Attack Type	**Naked-Eye Attack**				**Camera Attack**			
Number of User Operations	**1**	**2**	**3**	**5**	**1**	**2**	**3**	**5**
1 h	0	0	0	0	0	0	0	0
2 h	0	0	0	0	0	0	0	0
4 h	0	0	0	0	0	0	0	0
8 h	0	0	0	0	0	0	0	0
12 h	0	0	0	0	0	0	0	0

4.3.2. Smudge Attack

The experimental results of the smudge attacks are shown in Table 3, with 80 attacks and zero successes. The feedback received from the attackers is as follows: since the smudges left by the users were different each time, the specific information on the screen could not be accurately judged only from the smudges. Compared with traditional graphic-based login authentication schemes, PinWheel has significantly improved security [21].

Table 3. Experimental results of smudge attack.

Number of User Operations	1	2	3	5
1 h	0	0	0	0
2 h	0	0	0	0
4 h	0	0	0	0
8 h	0	0	0	0
12 h	0	0	0	0

4.3.3. Video Analysis Attack

The experimental results of the video analysis attacks are shown in Table 4, with 80 attacks and three successes. A video analysis attack is a malicious attack because attackers can obtain the login authentication process in the form of a video and review it repeatedly, which means that the attacker can obtain all the information on the user's login process clearly and easily. However, the success rate of the attack experiment was still not high.

Table 4. Experimental results of video analysis attack.

Scheme	PinWheel				THP [22]			
Number of User Operations	1	2	3	5	1	2	3	5
1 h	0	0	0	0	0	0	0	0
2 h	0	0	0	0	0	0	0	0
4 h	0	0	0	0	-	-	-	-
5 h	-	-	-	-	0	0	1	1
8 h	0	0	1	1	-	-	-	-
12 h	0	0	1	2	0	1	2	2

We proved that even if there are multiple screen authentication materials for login authentication, it is still difficult for an attacker to obtain the two challenge values passed by PinWheel in the first stage and the location selected by the user. Because there are many simultaneous possibilities, it makes analysis difficult to some extent.

As seen in Table 4, even if the comparison and inference can be performed through the user's multiple operations, a large amount of time is also consumed.

4.3.4. Comparisons

In the aspect of the experimental results, the attack success rate of the EvoPassscheme is 4% after three times of observation, and the attack success rate rises to 14% after four times of observation, while the attack success rate is 29% after five times of observation. For the TTUscheme, the probability of successful attack is less than 10%. In the video recording attack experiment, the success rate of the attack is more than 20%. In the experiment of shoulder-surfing attack, the rate of the normal PIN being successfully attacked is 10%. In the experiment of video recording attack, the probability of ColorPIN [23] being successfully cracked is higher than 80%. In PinWheel's attack experiment, when the attacker can observe three times, only video recording attacks succeeded twice. Overall, the attack success rate is 2/80. This means that PinWheel has better attack resistance. Therefore, PinWheel can resist shoulder-surfing attacks, smudge attacks, and video analysis attacks, so we believe that PinWheel has good security performance. In addition, users can also choose whether to add biometrics according to their needs, which also creates considerable protection of the PinWheel security.

5. User Study

In the user study, we recruited 573 subjects of different genders, ages, and occupations. We provided PinWheel guidelines for their use and conducted long-term observations on the use of these subjects. We designed a daily login time investigation for all subjects. PinWheel recorded the single unlock time of each subject daily using PinWheel to unlock the device, the type of PinWheel used, the total login time spent each day, and feedback data in the stages.

In addition, for ethical reasons, we did not observe users' private information. We considered this in the experimental scheme design, so we developed the PinWheel prototype used in the experiment to provide as much protection as possible for users' privacy. The identity information registered by the users was anonymous, and we only saved the data about the time for each login, the total daily login time, the registration time, the number of password resets, the use of extension schemes, and the questionnaires filled out by the users, which included basic information such as age, gender, and occupation. This information was only used as the basis for grouping the subjects when statistical experimental data were collected. These data were only used for the PinWheel user study, and before this experiment, we provided this explanation to each subject and explained that this allowed us to conduct further experiments after soliciting and obtaining their consent.

5.1. Investigation on Login Time

In this study, we had subjects in almost every age group for conducting the experiments, but in the process of data analyzing, we found that the data for users in some age groups were sometimes quite similar, so to facilitate readers being able to observe clearly, we integrated some data. For example, in the daily login time (the total length of time that the user device is on the PinWheel interface), we found that the login time curve for subjects aged 30–40 years and subjects aged 40–50 years were approximately the same, so the data were integrated. The result after integration is shown in Figure 5. For the age group corresponding to each curve, we first collected their daily login time data and performed the average calculation, which is the value corresponding to the curve. The purpose of our data design, such as the total daily login time, was to observe the time the subject spent on PinWheel every day. First, it was convenient for us to see if PinWheel consumes too much user time and causes difficulty for users (we also asked each user about this in the later investigative part of the questionnaire, and the result was positive). Second, it was convenient for us to understand the acceptance speed of PinWheel by users of different ages.

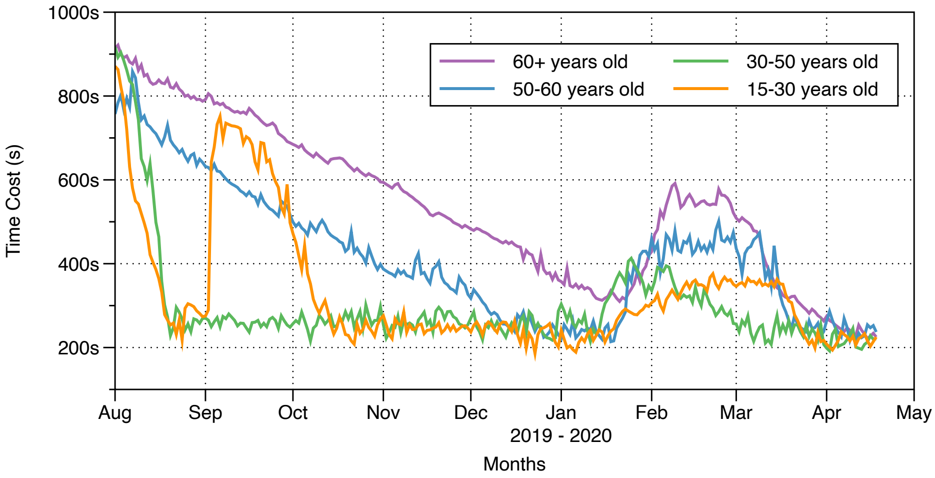
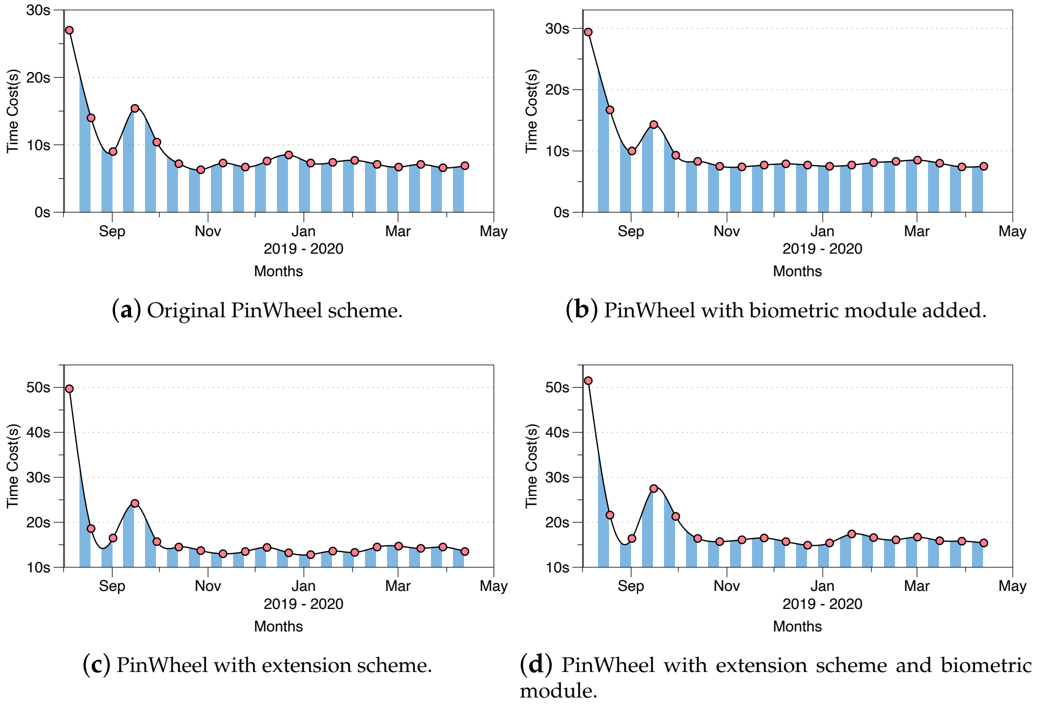


Figure 5. Total time consumed by users on PinWheel per day.

This experiment included data from all subjects using PinWheel, which means that it also included users who chose to use the PinWheel extension and users who used the biometric module. We explained the impact of the PinWheel expansion scheme and the biometrics scheme on the login time in subsequent experiments. We assumed that the number of times the subjects of the same age unlocked the mobile phone was approximately the same in a certain range. The data in Figure 5 reflect the time spent by the subjects on PinWheel's single login. It can be observed that in the early days of the experiment, subjects younger than 50 years old experienced a rapid decline in daily time, while subjects older than 50 years of age experienced a slow decline in daily login time. We believe that this is related to the acceptance and response speed of subjects of different ages (this is also reflected in the later questionnaire investigation).

It is worth mentioning that in September 2019, we added a new group of subjects, all of whom were 20–25 years old, which had a greater impact on the age curve. In addition, at the beginning of 2020, the time curve corresponding to each age group had an upward trend. We carefully investigated the data during this period and found that there was no significant change in the single login time of the subjects, and the single number of mobile phone unlocks per day increased slightly.

Since users chose to use PinWheel in different ways, for example, in addition to the initial PinWheel program and to respond to different security requirements, we also provided users with optional expansion programs and biometric modules. This created diversity in users' choices, and there were also certain differences in use, which was mainly reflected in the time required for login authentication; therefore, we focused on the difference in login time for users who chose different PinWheel extension solutions. In Figure 5, we grouped by the age of the subject to observe the acceptance speed of PinWheel by subjects of different ages. However, in Figure 6, we focused on the changing trend in authentication time during the long-term use of PinWheel and its extension solutions. We believe that this also changed the difficulty of different expansion schemes in daily use to some extent. In Figure 6, we no longer distinguish subjects by age, but divide the subjects into four groups according to the choice of program: Figure 6a represents the users who selected the original PinWheel, Figure 6b the users who selected the biometric module for assistance, Figure 6c the users who selected the expansion scheme to add the number of beads, and Figure 6d the users who added a biometrics module and an extended solution to the original PinWheel. We summarized the data of these users each time they logged in and performed average calculations each day. To make the data clearer, we took the data every two weeks and used them as a representative to draw a statistical chart. In other words, Figure 6 reflects the change in the average daily login time of the four users in the eight month long-term experiment. After using the original PinWheel program for a period of time, the average login time was approximately 7-9 s, the average login time of the last three programs under long-term use was 8 s, 14 s, and 17 s, and the average subject used PinWheel to unlock approximately 42 times a day. This was slightly longer than the average login time of traditional text passwords or graphic passwords, but shorter than other similar schemes [18,22,24], and PinWheel had better security.



(**a**) Original PinWheel scheme.

(**b**) PinWheel with biometric module added.

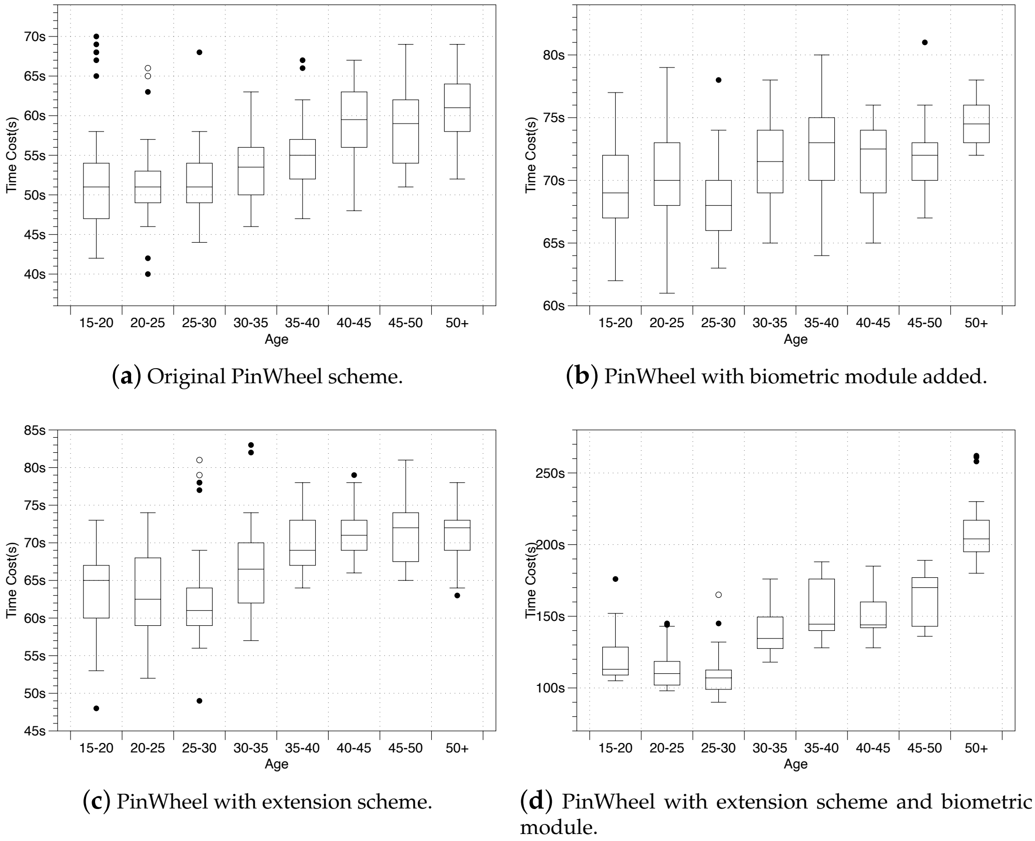
(**c**) PinWheel with extension scheme.

(**d**) PinWheel with extension scheme and biometric module.

Figure 6. The impact of different PinWheel extension schemes on authentication time.

5.2. *Investigation of Registration Time*

We also focused on the PinWheel registration time. We believe that in a certain sense, the time spent on user registration can also reflect the speed of user acceptance of PinWheel so that we can understand the actual performance of PinWheel. We still performed age stratification for users and differentiated statistics according to the type of user selection scheme. The types of schemes here refer to the original PinWheel and the PinWheel with added extension schemes, which were divided into four categories: (1) original PinWheel, (2) added biometrics on the basis of the original PinWheel, (3) added bead number on the basis of the original PinWheel and the password length becoming three digits, and (4) added bead number on the basis of the original PinWheel, the password length becoming three digits, and biometrics technology was used. We carried out the statistics of the registration time for the users who chose the above four schemes, and the results are shown in Figure 7. Figure 7a–d corresponds to the above four cases in order. It can be observed that the average registration time of users using the original PinWheel was between 50 and 60 s, and after adding the number of beads or adding biometric technologies, the registration time increased by approximately 15 s on average. If users added the number of beads and biometric technologies, the registration time could exceed 120 s, and it differed considerably between different age groups. We speculate that this is related to the cumbersome registration process, which is worth improving in the future. We also noticed that for users over 45 years of age, the registration time was relatively high. However, one of the interesting things is that we also asked users in the questionnaire whether they were annoyed by the long registration process, and most of them said they could accept it.



(**a**) Original PinWheel scheme.

(**b**) PinWheel with biometric module added.

(**c**) PinWheel with extension scheme.

(**d**) PinWheel with extension scheme and biometric module.

Figure 7. Registration time.

5.3. Investigation on Users' Preference

In the attack experiment in Section 4, we mentioned that in crowded places, the probability of shoulder-surfing attacks is very high. Therefore, in the questionnaire investigation, we collected whether the user could focus on shoulder-surfing attacks in different scenarios, which we named in the preference investigation. We assumed a total of 14 scenarios: home, restaurant, shopping mall, company/lab, subway/bus, library, square, street, plane/train, classroom, cafe, station/airport, gymnasium, and hotel, and we also counted the feedback results of users of different ages, as shown in Figure 8. It can be clearly observed that 15–30-year-old subjects had a clear understanding of the risk of password exposure caused by shoulder-surfing attacks. In most scenarios, they believed that corresponding measures should be performed to protect their privacy information for login authentication. However, in the group of subjects over 30 years of age, the risks posed by shoulder-surfing attacks did not receive enough attention. In particular, users over 40 years old were almost indifferent to the risks posed by shoulder-surfing attacks. We believe that these people should strengthen their awareness of protecting their privacy.

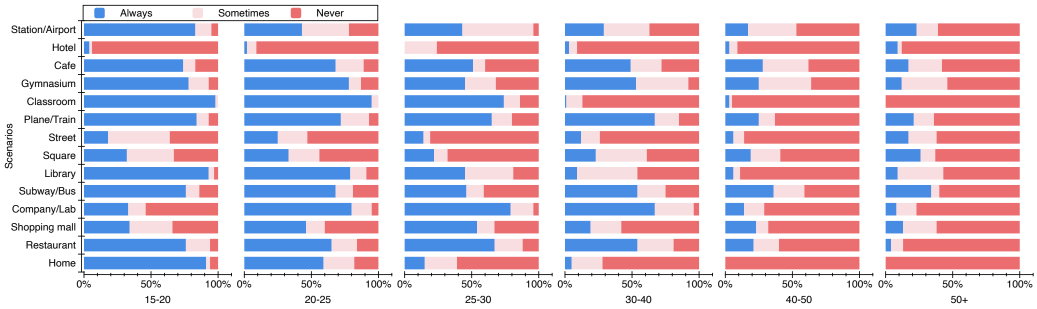


Figure 8. Survey of usage habits.

In 14 scenarios, most users chose to ignore two scenarios: street and hotel. We think this is also where users need to improve their awareness because streets and hotels also have the risk of malicious cameras conducting shoulder-surfing attacks to obtain users' privacy. Scenarios such as classroom and lab were strongly related to occupation and age, so the distinction of users' preferences was more obvious in Figure 8. In this experiment, the majority of students in the 15–25 age group were college students, so the experimental results had some limitations. We also hope to make up for this in our future work.

In addition to the above preference investigation, we also investigated the user's preference regarding PinWheel usage scenarios. We simulated 12 scenarios involving privacy information commonly used in life for users and provided users with six options to see if users think PinWheel should be used in these scenarios to improve security (see the Appendix for the questionnaire). The results are shown in Figure 9. It can be seen that for company website, daily mobile payment, etc., users preferred not to use PinWheel. For some scenarios with high security requirements, such as smart safety box, asset management, and control center, users preferred to use PinWheel to improve their security, which is in line with our expectations. We believe that PinWheel is slightly worse than traditional text passwords and graphic passwords in unlocking speed and convenience, but in exchange for a considerable improvement in security. This plays an important role in protecting important private information from threats such as shoulder-surfing attacks.

5.4. Investigation on Users' Feedback

In the questionnaire, based on users' feedback, we attempted to answer some of our general questions based on the feedback data: for PinWheel and extension solutions for PinWheel,

- Is it considered safe?
- Does it affect user requirements for convenience?
- Are users satisfied with the speed of login authentication?
- Are users satisfied with compatibility? Does it crash, etc. ?
- Is the password difficult to remember?

We asked the subjects participating in the questionnaire to evaluate the five questions in the form of scores. We summarized these problems as the five performance criteria of the program: safety, convenience, speed, stability, and memorability. We took the average of male and female users of different ages, so for each performance criterion, we obtained 16 scores. Figure 10 shows the results of this investigation. In Figure 10, the blue points represent the PinWheel original solution, and the red points represent the PinWheel extension solutions (including bead number expansion and biometrics).

We also calculated the mean value for the results of each performance. It can be seen that most of the subjects believe that the PinWheel scheme is sufficiently safe, and the extension solutions can improve PinWheel's safety. In addition, PinWheel also performs well in terms of stability and memory. In terms of convenience and speed, users maintained an average level of 75–85, which shows that PinWheel is more suitable for places with high security requirements, at the expense of convenience and speed, in exchange for security improvements. We also recommend this choice. In the experiment in Figure 10, in order to more clearly reflect the user's views on the scheme, we did not use dualism (agree or disagree), but used the form of scoring in the questionnaire. In order to compare with TTU and other schemes, we regarded 85 points or more as a positive attitude and 85 points or less as a negative attitude. The comparison results are shown in Table 5. It can be seen that PinWheel has better user evaluation in terms of security and memory. We calculated statistics for the participants of the user study, including their basic information, as well as part of the information in the questionnaire, which are shown in Appendix A.

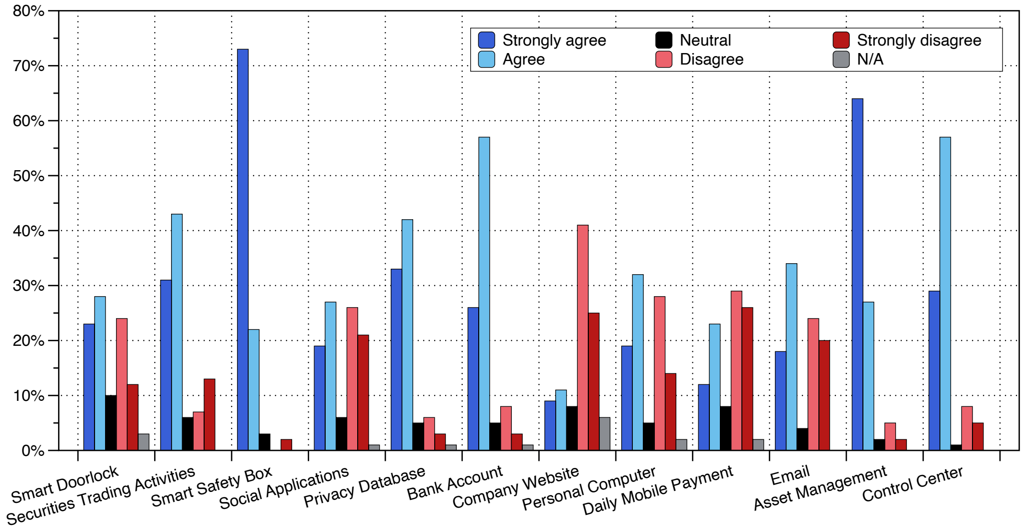


Figure 9. Survey on users' preference for PinWheel application scenarios.

Table 5. The comparison of usability index.

	Safety	Convenience	Speed	Stability	Memorability
ColorPIN	91.7%	4.2%	-	-	54.2%
BWPIN	37.5%	37.5%	-	-	-
TTU	62.5%	20.8%	87.5%	-	-
Normal PIN	20.8%	54.1%	-	-	37.5%
PinWheel	100%	43.3%	12.0%	100%	73.6%

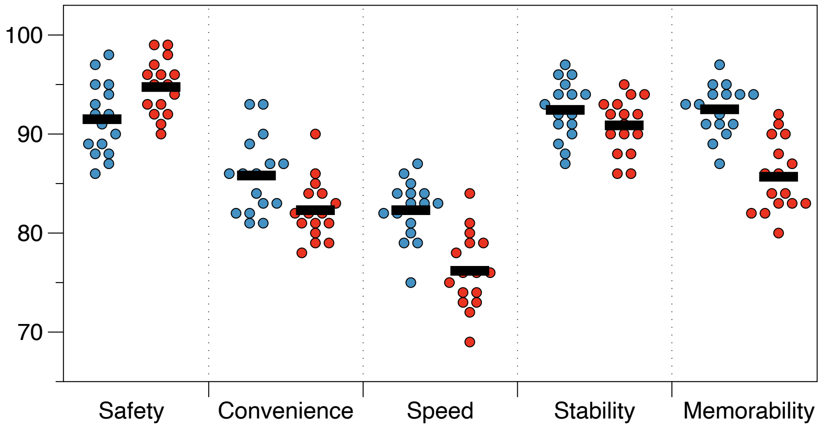


Figure 10. Observing the average score of PinWheel in the user survey from five aspects.

6. Security Analysis

6.1. Random Guess Attacks

The attacker attempts to log in at the second stage of the login process of PinWheel, trying to crack PinWheel by random guessing. We do not discuss the first stage of login, because we think that the attacker cannot get any valid information in the first stage if he/she does not obtain prior knowledge about the user's password. The key factor affecting PinWheel's resistance to random guessing attack is the number of beads selected by users. To quantify the security of PinWheel against random guess attacks, we define the entropy of a password space as follows:

$$Entropy = \log_2 \{\tbinom{36}{n} \cdot n!\} \tag{1}$$

If the entropy of a password space is x bits, there will be 2^x possible passwords in that space. Parameter n is the number of beads selected by the user. Table 6 shows the entropies of PinWheel and PassMatrix [25], as well as the corresponding entropies of text passwords and PIN passwords. It is worth mentioning that the PassMatrix scheme also includes the expansion part. The data in Table 6 include the original PassMatrix and the expansion scheme of PassMatrix. We compare PinWheel and PassMatrix from their basic schemes (n = 1) and gradually increase the value of n. It can be seen that under the same conditions, when $n \leq 4$, the entropy of PinWheel is larger than that of PassMatrix, and when $n \leq 3$, it has a larger entropy than that of text passwords. This means that under the same conditions, PinWheel has better resistance to a random guess attack. However, we do not think PinWheel is good enough in this aspect. Our main focus is shoulder-surfing attack, smudge attack, and video analysis attack. As for other reasonable limitations, we will discuss these in Section 7.

Table 6. The comparison of entropy.

n (Expansion Level of the Scheme)	1	2	3	4	5
PinWheel	10.3	15.4	20.4	25.4	30.3
PassMatrix	6.3	12.6	18.8	25.0	31.3
Text Passwords	6.6	13.1	19.7	26.3	32.9
PIN	3.3	6.6	10.0	13.3	16.6

7. Discussion

In the attack experiment, we tested several mainstream attack methods for PinWheel to show PinWheel's resistance. It can be seen that the effect of the attack on it is poor. We think this is related to PinWheel's design logic. In the shoulder-surfing attack experiment, most of the subjects who played the attacker believed that the effective information on the screen could not be effectively obtained during a shoulder-surfing attack, and some attackers also believed that because the user's operation was relatively fast, it added difficulty to the attack. In the video analysis attack experiment, some attackers said that even if the user's login process could be clearly obtained, it would still be difficult to effectively analyze the password because the combination of beads and areas varies.

PinWheel's purpose is to balance the ability to resist attacks and user convenience. We carefully considered the association and difference between the user's action to distinguish valid information and exclude irrelevant information during the login process and the attacker's action to obtain valid information. We want to create a scheme that is user-friendly and that the attacker feels is difficult, instead of focusing only on security but at the expense of users' usability.

In the smudge attack experiment, we also proved the resistance of PinWheel in the face of a smudge attack. Because the challenge value is refreshed randomly during each login, the length of the trace left on the screen is different for each login operation by the user. Because of this, the profit of the smudge attack is also very small.

Limitations: Although PinWheel performs well in terms of security, we believe that PinWheel still has some inherent defects. First, PinWheel's interface would cause difficulty for individuals with color blindness. We did not take this into consideration when we originally designed it, and we plan to improve this problem in a later updated version. Second, PinWheel is also affected by random guessing attack. In the user study, we also found that many users prefer to choose the location of the bead and area that are easy to remember, for example located at the top or bottom of the interface, which could inevitably become a hotspot for attackers. However, we also believe that the combined password between bead and area has a low probability of being guessed by a hotspot attack. In other words, this is still a major challenge for attackers. In addition to exploring improvement strategies in the scheme, we also hope that users can proactively avoid hotspot attacks during registration.

8. Conclusions

In this paper, we develop a new authentication scheme that can protect users' passwords even under shoulder-surfing attacks. Our PinWheel combines graphics-based and text-based passwords to achieve two goals: high security and high usability. The high security is due to the design, which implicitly passes the challenge values to the user, which makes our method resistant in a majority of attacks, even video analysis attacks. The high usability benefits from the graphic-based scheme, which is easy to remember. We implemented the prototype of the PinWheel scheme on Android and iOS platforms and conducted attack experiments and user studies to comprehensively evaluate the scheme performance. Our evaluation involved 573 participants over 262 days. The experimental results demonstrate the high security and usability of our scheme. Furthermore, we theoretically analyzed the security of PinWheel and then proposed an extension scheme that allows users to dynamically set their passwords to meet various security requirements in different scenarios. It was also shown to be effective. In the future, we plan to add support for color blind patients and continue to optimize the user experience.

Author Contributions: Conceptualization, Y.L.; methodology, Y.L.; software, Y.L. and X.Y.; validation, L.F., C.G., and Y.L.; investigation, X.Y.; resources, L.F.; data curation, C.G.; writing, original draft preparation, Y.L.; writing, review and editing, Y.L. and X.Y.; supervision, L.F. and C.G.; funding acquisition, L.F. All authors read and agreed to the published version of the manuscript.

Funding: This research was funded by National Key R&D Program of China (Grant No.2020AAA0107703), and National Natural Science Foundation of China (Grant No. 62032025, 62076125, 61872181, U20B2049, U20B2050, 61702236), and National Key R&D Program of China (Grant No.2020YFB1005902).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study. Written informed consent has been obtained from the subjects to publish this paper.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Appendix A.1. Full Descriptions of Participants and Votes

We performed statistics on the participants of user study. In addition to age, gender, occupation, and other basic information statistics, this also includes the correlation between them and some experimental data. The details of this part are shown in Table A1.

Appendix A.2. Investigation Instrument

Introduction Thank you for your support of PinWheel user usability experiment. As these choices may have positive or negative consequences, which will have an huge impact on our research, please fill in carefully according to the actual situation.

Privacy statement This survey is completed anonymously. We promise that the above private information (including gender, occupation, etc.) will only be used for research purposes.

Participation should take about 10 min.

What is your age range? ○15–30 ○30–50 ○50–60 ○60+

What is your gender? ○Male ○Female

What is your occupation? ○Please answer: ____________

Did you choose the extension scheme and biometric module? ○Yes, I chose the extended solution or the biometric module or both ○ No, just chose the original PinWheel scheme

Please give a reasonable score for the following questions, the score range is 0–100:

- What do you think of the security of the PinWheel?
  ○Score: ____________
- Do you think that the PinWheel is very stable (no crashes, no passwords, cannot login smoothly with the correct password, etc.)? ○Score: ____________
- Are you satisfied with the login authentication speed of the PinWheel program? ○Score: ____________
- Do you think the PinWheel meets the user′s convenience requirements? ○Score: ____________
- Do you think the password of PinWheel is difficult to remember? ○Score: ____________

Do you think the password of Pinwheel can be easily guessed? ○Yes ○No

Do you think Pinwheel's login process is troublesome? ○Yes ○No

Do you think PinWheel can be improved? ○Yes ○No

Would you pay attention to shoulder-surfing attack by others in the following scenarios? Or in these scenarios, when performing mobile device login authentication, would you be vigilant and try to avoid others obtaining the password? 1. Home 2. Restaurant 3. Shopping Mall 4. Company/Lab 5. Subway/Bus 6. Library 7. Square 8. Street 9.Plane/Train 10. Classroom 11. Gymnasium 12. Cafe 13. Hotel 14. Station/Airport
○Always ○Sometimes ○Never

Are you annoyed by the long registration time?
○Yes ○No

Has the time consumed by the PinWheel login process caused problems in your daily life?
○Yes ○No

Are you willing to choose PinWheel in the following scenarios sensitive to privacy data to reduce the risk of being attacked and protect privacy? 1. Smart Doorlock 2. Securities Trading Activities 3. Smart Safety Box 4. Social Applications 5. Privacy Database 6. Bank Account 7. Company Website 8. Personal Computer 9. Daily Mobile Payment 10. Email 11. Asset Management 12. Control Center
○Strongly Agree ○Agree ○Neutral ○Strongly Disagree ○Disagree ○N/A

Please select the extension scheme and the biometric module users to answer the following questions (only users who choose the original PinWheel plan can choose not to answer):

- Do you think that the extension scheme and biometrics module have caused trouble for the login authentication process? ○Yes ○No
- Do you think the extension scheme and biometric module have a positive impact on security? ○Yes ○No

Table A1. Full descriptions of participants and votes.

	Population Distribution		Agree with Its Security		Agree with Its Stability		Agree with Its Convenience		Easy to Remember	
	No.	**Prop.**	**No.**	**Prop.**	**No.**	**Prop.**	**No.**	**Prop.**	**No.**	**Prop.**
Age	**573**	**100%**	**557**	**97.2%**	**569**	**99.3%**	**534**	**93.2%**	**517**	**90.2%**
15–30	262	45.7%	251	95.8%	259	98.9%	258	98.5%	251	95.8%
30–50	187	32.6%	182	97.3%	186	99.5%	159	85.0%	160	85.6%
50–60	110	19.2%	110	100%	110	100%	105	95.5%	97	88.2%
60+	14	2.4%	14	100%	14	100%	12	85.7%	9	64.3%
Gender	**573**	**100%**	**557**	**97.2%**	**569**	**99.3%**	**534**	**93.2%**	**517**	**90.2%**
Male	292	51.0%	283	96.9%	290	99.3%	274	93.8%	260	89.0%
Female	271	47.3%	264	97.4%	269	99.3%	251	92.6%	248	91.5%
Non-binary	0	0.0%	0	100.0%	0	100.0%	0	100.0%	0	100.0%
Other	1	0.2%	1	100%	1	100%	1	100%	1	100%
Prefer not to say	9	1.6%	9	100%	9	100%	8	88.9%	8	88.9%
Occupation	**573**	**100%**	**557**	**97.2%**	**569**	**99.3%**	**534**	**93.2%**	**517**	**90.2%**
Student	267	46.6%	256	95.9%	266	99.6%	248	92.9%	249	93.3%
Teacher	12	2.1%	8	66.7%	12	100%	8	66.7%	7	58.3%
Social elite	294	51.3%	293	99.7%	291	99.0%	278	94.6%	261	88.8%
Phone brand	**573**	**100%**	**557**	**97.2%**	**569**	**99.3%**	**534**	**93.2%**	**517**	**90.2%**
iPhone	87	15.2%	83	95.4%	87	100%	78	89.7%	80	92.0%
HUAWEI	89	15.5%	85	95.6%	89	100%	86	96.6%	77	86.5%
OPPO	41	7.2%	40	97.6%	40	97.6%	38	92.7%	35	85.4%
VIVO	52	9.1%	52	100%	52	100%	45	86.5%	48	92.3%
XIAOMI	95	16.6%	93	97.9%	94	98.9%	87	91.6%	89	93.7%
Samsung	58	10.1%	56	96.5%	58	100%	52	89.7%	52	89.7%
Others	151	26.4%	148	98.0%	149	98.7%	148	98.0%	136	90.0%
Scheme	**573**	**100%**	**557**	**97.2%**	**569**	**99.3%**	**534**	**93.2%**	**517**	**90.2%**
Original scheme	422	73.6%	408	96.7%	422	100.0%	407	96.5%	413	97.9%
Extension scheme	66	11.5%	64	97.0%	65	98.5%	54	81.8%	42	63.6%
Biometric module	53	9.2%	53	100.0%	52	98.1%	46	86.8%	49	92.5%
Both have chosen	32	5.6%	32	100.0%	30	93.8%	27	84.4%	13	40.6%
Login Time	**573**	**100%**	**557**	**97.2%**	**569**	**99.3%**	**534**	**93.2%**	**517**	**90.2%**
5–10 s	475	82.9%	465	97.9%	472	99.4%	448	94.3%	429	90.3%
11–20 s	98	17.1%	92	93.9%	97	99.0%	86	87.8%	88	89.8%
21–30 s	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
30 s+	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Registration Time	**573**	**100%**	**557**	**97.2%**	**569**	**99.3%**	**534**	**93.2%**	**517**	**90.2%**
40–100 s	544	94.9%	533	98.0%	540	99.3%	522	96.0%	504	92.6%
100–150 s	7	1.2%	6	85.7%	7	100.0%	4	57.1%	5	71.4%
150–200 s	14	2.4%	11	78.6%	14	100.0%	6	42.9%	6	42.9%
200 s+	8	1.4%	7	87.5%	8	100.0%	2	25.0%	2	25.0%

References

1. Sepideh, F. Providing a Secure Hybrid Method for Graphical Password Authentication to Prevent Shoulder Surfing, Smudge and Brute Force Attack. *Int. J. Comput. Inf. Eng.* **2019**, *13*, 616–620.
2. Harbach, M.; Von Zezschwitz, E.; Fichtner, A.; De Luca, A.; Smith, M. It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In Proceedings of the 10th Symposium On Usable Privacy and Security ({SOUPS} 2014), Menlo Park, CA, USA, 9–11 July 2014; pp. 213–230.
3. Vaddeti, A.; Vidiyala, D.; Puritipati, V.; Ponnuru, R.B.; Shin, J.S.; Alavalapati, G.R. Graphical passwords: Behind the attainment of goals. *Secur. Priv.* **2020**, *3*, e125. [CrossRef]
4. Li, X.; Zhu, Y.; Wang, J.; Liu, Z.; Liu, Y.; Zhang, M. On the soundness and security of privacy-preserving SVM for outsourcing data classification. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 906–912. [CrossRef]

5. Rechavi, A.; Berenblum, T. What's in a Name? Using Words' Uniqueness to Identify Hackers in Brute Force Attacks. *Int. J. Cyber Criminol.* **2020**, *14*, 361–382.
6. Tank, H.; Harsora, V. A Survey on Secure Virtual Password and Phishing Attack. In Proceedings of the 4th International Conference on Computer Science and Information Technology (ICCIT 2015), Gujarat, India, 1–2 April 2015; pp. 1–15.
7. Guo, Y.; Zhang, Z.; Guo, Y. Optiwords: A new password policy for creating memorable and strong passwords. *Comput. Secur.* **2019**, *85*, 423–435. [CrossRef]
8. Varshney, S.; Umar, M.S.; Nazir, A. A Secure Shoulder Surfing Resistant Hybrid Graphical User Authentication Scheme. In *Cybernetics, Cognition and Machine Learning Applications*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 79–87.
9. Katsini, C.; Fidas, C.; Belk, M.; Samaras, G.; Avouris, N. A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication. *Int. J. Hum. Comput. Interact.* **2019**, *35*, 1800–1812. [CrossRef]
10. Yee, L.; Ku, C.S.; Ang, T.F. Preventing Shoulder-Surfing Attacks using Digraph Substitution Rules and Pass-Image Output Feedback. *Symmetry* **2019**, *11*, 1087.
11. Alsuhibany, S.A. Usability and shoulder surfing vulnerability of pattern passwords on mobile devices using camouflage patterns. *J. Ambient Intell. Humaniz. Comput.* **2019**, *11*, 1645–1655. [CrossRef]
12. De Luca, A.; Von Zezschwitz, E.; Nguyen, N.D.H.; Maurer, M.E.; Rubegni, E.; Scipioni, M.P.; Langheinrich, M. Back-of-device authentication on smartphones. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Paris, France, 27 April–2 May 2013; pp. 2389–2398.
13. Von Zezschwitz, E.; De Luca, A.; Brunkow, B.; Hussmann, H. Swipin: Fast and secure pin-entry on smartphones. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, 18–23 April 2015; pp. 1403–1406.
14. Saad, A.; Chukwu, M.; Schneegass, S. Communicating Shoulder Surfing Attacks to Users. In Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia, Cairo, Egypt, 25–28 November 2018; pp. 147–152.
15. Schneegass, S.; Oualil, Y.; Bulling, A. SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 7–12 May 2016; pp. 1379–1384.
16. Wu, T.S.; Lee, M.L.; Lin, H.Y.; Wang, C.Y. Shoulder-surfing-proof graphical password authentication scheme. *Int. J. Inf. Secur.* **2014**, *13*, 245–254. [CrossRef]
17. Zhou, Z.; Yang, C.N.; Yang, Y.; Sun, X. Polynomial-based Google map graphical password system against shoulder-surfing attacks in cloud environment. *Complexity* **2019**, *2019*, 2875676. [CrossRef]
18. Chen, S.; Zhu, Y. A Textual Password Entry Method Resistant to Human Shoulder-Surfing Attack. In *International Symposium on Cyberspace Safety and Security*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 409–420.
19. Yu, X.; Wang, Z.; Li, Y.; Li, L.; Zhu, W.T.; Song, L. EvoPass: Evolvable graphical password against shoulder-surfing attacks. *Comput. Secur.* **2017**, *70*, 179–198. [CrossRef]
20. Nyang, D.; Kim, H.; Lee, W.; Kang, S.b.; Cho, G.; Lee, M.K.; Mohaisen, A. Two-Thumbs-Up: Physical protection for PIN entry secure against recording attacks. *Comput. Secur.* **2018**, *78*, 1–15. [CrossRef]
21. Ali, A.; Rafique, H.; Arshad, T.; Alqarni, M.A.; Chauhdary, S.H.; Bashir, A.K. A fractal-based authentication technique using sierpinski triangles in smart devices. *Sensors* **2019**, *19*, 678. [CrossRef]
22. Fang, L.; Li, Y.; Yun, X.; Wen, Z.; Tanveer, M. THP: A Novel Authentication Scheme to Prevent Multiple Attacks in SDN-based IoT Network. *IEEE Internet Things J.* **2019**. [CrossRef]
23. De Luca, A.; Hertzschuch, K.; Hussmann, H. ColorPIN: Securing PIN entry through indirect input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, GA, USA, 10–15 April 2010; pp. 1103–1106.
24. Panda, S.; Kumari, M.; Mondal, S. SGP: A Safe Graphical Password System Resisting Shoulder-Surfing Attack on Smartphones. In *International Conference on Information Systems Security*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 129–145.
25. Sun, H.M.; Chen, S.T.; Yeh, J.H.; Cheng, C.Y. A Shoulder Surfing Resistant Graphical Authentication System. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 180–193 [CrossRef]