Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 8019830, 9 pages
http://dx.doi.org/10.1155/2016/8019830

Research Article

Enhancing the Security of Personal Identification Numbers with Three-Dimensional Displays

Mun-Kyu Lee,[1] Jin Bok Kim,[2] and Matthew K. Franklin[3]

[1]*Department of Computer and Information Engineering, Inha University, Incheon 402-751, Republic of Korea*
[2]*Kakao Corporation, Jeju 63309, Republic of Korea*
[3]*Department of Computer Science, UC Davis, CA 95616, USA*

Correspondence should be addressed to Mun-Kyu Lee; mklee@inha.ac.kr

Received 28 October 2015; Accepted 20 March 2016

Academic Editor: Ching-Hsien Hsu

Passwords and personal identification numbers (PINs) are convenient and ubiquitous, but they are quite vulnerable to attackers who stand near the user ("shoulder-surfers"). This problem may be partially resolved by changing the user interface, but previous solutions of this kind still give shoulder-surfing attackers a significant advantage over brute force search. This paper provides a novel solution based on three dimensions, particularly suitable for glasses-free three-dimensional (3D) displays found in many smartphones and handheld game consoles. A user at the "3D spot" may log in easily, while nearby shoulder-surfers gain no advantage. A detailed experimental usability analysis is performed to demonstrate the effectiveness of the proposed scheme in comparison to the existing methods.

1. Introduction

User authentication is a procedure that enables a user of a system to prove his or her identity and to access the system. Although there are various approaches to user authentication [1, 2], the practical reality is that authentication based on the user's memory is still used in a majority of cases [3]. For example, passwords are frequently used to access desktop personal computers, terminals, and websites, and personal identification numbers (PINs) are used to withdraw cash from an automated teller machine (ATM), unlock a mobile device, and even open a door. While there have been various efforts to improve the security of passwords and PINs by helping users choose good ones and keep them secret; for example, [3–5], the essential problem of passwords and PINs is that they are vulnerable to shoulder-surfing attacks. In other words, anyone who observes the log-on procedure can easily memorize the password after looking over the user's shoulder [6].

One direction of research in the literature to solve this problem is to revise the interface to input a password or PIN [6]. That is, instead of entering directly the secret itself, the user is given randomized challenges and is asked to input appropriate responses that are computed using the password or PIN. The challenge-response task should be designed in an asymmetric manner so that the user may easily compute the responses, while the observer may not obtain useful information on the secret by observing a session. For example, the binary PIN-entry method [6] modifies the regular PIN pad and displays digits with black and white background colors as a challenge. The user recognizes the color of the current PIN digit and touches one of the two keys, "Black" and "White." To uniquely determine a PIN digit, this task is iterated four times, requiring 16 stages in total to input a 4-digit PIN. Figure 1 shows an example wherein "1" is being inputted via this method over a smartphone.

However, the modification of the input interface does not solve the problem completely. Because the attacker observes the challenge-response pairs, s/he may get partial information on the secret, if not the whole PIN. Moreover, if the attacker is helped by additional material such as a recording device, the attack will be much easier. For example, an

Figure 1: Example round to input "1" in the binary PIN-entry method [6] (reproduction of Figure 1 in [7]). The user enters "Black," "Black," "White," and "White" in sequence. (a) Stage 1. (b) Stage 2. (c) Stage 3. (d) Stage 4.

attacker against the above binary method [6] can determine the PIN uniquely if s/he can record all challenge-response pairs.

Therefore, a more promising solution is to physically prevent an attacker from observing an input session [7]. This may be realized using secure secondary channels such as an audio channel [9, 10] and a vibration channel [9–13] that are not accessible by the attacker. In these methods, the challenge transmitted through secondary channels is combined with the information shown over the open visual channel. That is, they are multimodal methods. However, it is known that unimodal performance is much better than multimodal performance [14], and the visual channel is still the most effective data transmission channel because about 80% of the information that we obtain comes through our eyes [15].

Then, a natural question would be "can we construct a *secure* visual channel?" In this paper, an affirmative answer to this question is given, and a secure PIN-entry method using a three-dimensional (3D) display is presented. In the proposed method called *3DPIN*, the random challenge is displayed to the user as a stereoscopic image. An attacker who does not have access to the 3D channel obtains no information on the challenge. The proposed method is particularly useful for glasses-free 3D displays such as parallax barrier displays [16] used in various smartphones and handheld game consoles. The 3D challenge is only visible to the legitimate user who is at a specific spot in front of the display, which we call the *3D spot*, while the attacker who is located in any other spot does not recognize the 3D effect. In a setting with 3D glasses such as a shutter system or a polarization system, the legitimate user who wears the 3D glasses can recognize the 3D challenge, but any person who does not wear the glasses cannot.

A part of this paper was presented at GCCE 2014 [8]. In this extended version, more technical details for the design of 3DPIN and realization of 3D effects are provided. In addition, the results of enhanced performance analyses are explained. Finally, the security against a brute force attack and a shoulder-surfing attack is analyzed in comparison to the existing methods.

2. 3DPIN

Figure 2 shows the layout of the proposed method, 3DPIN. Although the proposed method was implemented and tested over a smartphone that employs the parallax barrier display for 3D effects, we modified the screenshots so that the readers may understand the concept by using easily accessible anaglyph glasses with red (left eye) and cyan (right eye) filters. That is, each digit was modified to have two components with red and cyan colors. If the reader looks at the figures through the anaglyph glasses, it gives similar effects to the situation where the reader is at the 3D spot in front of the smartphone. For example, "8" has a different depth from the other digits, as shown in Figure 2(b), because the red and cyan components are in the opposite direction of each other as compared to the other digits. However, it should be noted that this does not imply that the reader's view without the anaglyph glasses is equivalent to the attacker's view who is at a wrong position with respect to the smartphone. Because the red and cyan figures are displayed in black in the real smartphone implementation, as shown in Figure 4, a prominent digit and a depressed digit look the same in two-dimensional (2D) vision. That is, the attacker who is not at the 3D spot sees either ten digits with the same depth or ten blurred digits.

The basic principle of the proposed method is similar to that of a traditional safe with a dial lock. That is, the user is required to enter a PIN digit by rotating it and aligning it with an indicator symbol. However, a few novel techniques were used in the design of the proposed method as follows:

(i) Phantom indicator: in the proposed method, there is no explicit indicator such as an arrow or a marker on a dial lock. It is sufficient that one random digit

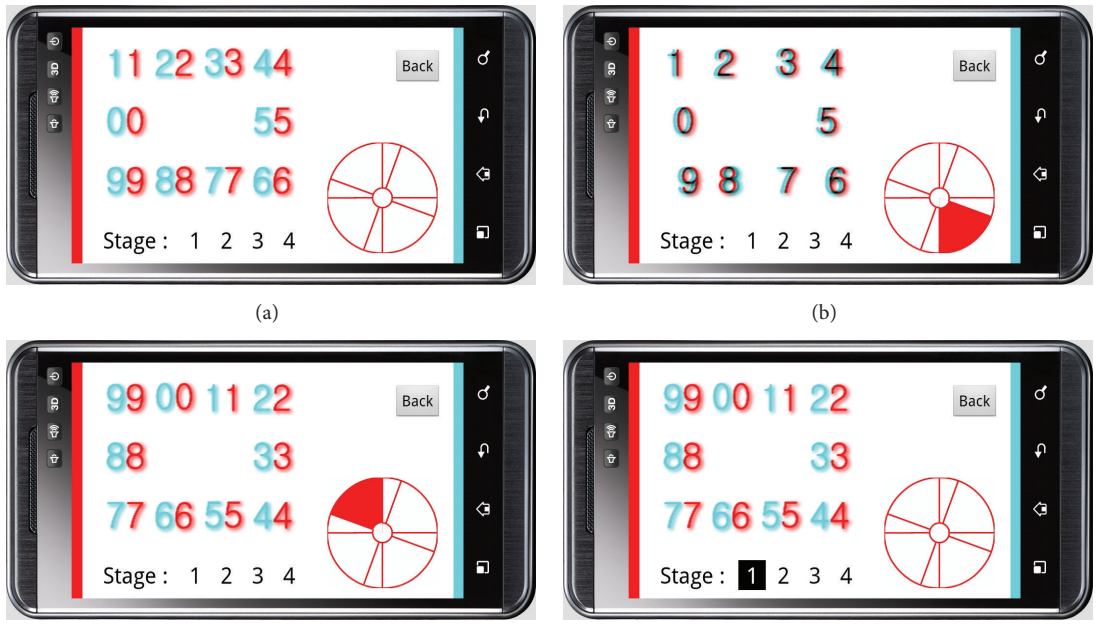

FIGURE 2: Example procedure for one digit entry using the proposed method (reproduction of Figure 1 in [8]). (a) Initial state. (b) Challenge transmission. (c) Commitment of response. (d) Next digit.

is displayed with a different depth from those of the others. For example, in a challenge given in Figure 2(b), the position of "8" is remembered as a phantom indicator. For the sake of convenience, we will call "8" an indicator digit in this case. The user's task is to align the target PIN digit with the phantom indicator by rotating the digit array. For maximum security, we designed the method so that the depth is displayed for a minimum time and all digits become located in the same layer (as shown in Figure 2(c)) right after the user starts rotation.

(ii) Rectangular arrangement: the digits are arranged as a 3×4 array as shown in Figure 2(a), not as a circle, because we found out from a pilot test that the users better recognize the depth of each digit when the digits are arranged in a rectangular form than when they are in a circular or diamond arrangement.

(iii) Position perturbation: when the digits are displayed in three dimensions, as shown in Figure 2(b), the horizontal position of each digit is slightly perturbed for security reasons. The principle of 3D displays is to show different images to the left and right eyes. Figures 3(a) and 3(b) are the simulated images shown to the left and right eyes, respectively, when there is no position randomization. When the user who is at the 3D spot sees the image shown in Figure 3(c), the attacker who is not at the right position may see the image in either Figure 3(a) or Figure 3(b). Whereas the distances between the adjacent digits in Figure 3(c) are the same, they are different in Figures 3(a) and 3(b). That is, "9," which is a prominent digit in the 3D image, has a relatively shifted position in the separated image for each eye. This may reveal the indicator to the attacker. We solve this problem by slightly moving each digit horizontally by a random amount.

(iv) Indirect touch: in order to rotate the digit array, the user does not directly touch the digits but uses the scroll wheel displayed at the right bottom corner of the touch screen. This indirect interface enhances security, because the users tend to directly touch the correct PIN digit unconsciously if they are allowed to touch the rectangular dial.

As a result of adopting the above four techniques, the proposed method works as follows: initially, the rectangular array is displayed as shown in Figure 2(a). All digits are displayed at the same depth. At the moment the user puts his/her finger on the scroll wheel, the touched region in the wheel changes red and the digits change their depth. The phantom indicator digit, for example, "8" in Figure 2(b), is displayed as a prominent object and the other digits are displayed as depressed objects, or vice versa. After the user recognizes the phantom indicator, s/he scrolls the wheel to rotate the array if needed. For example, if the user wants to input "6," s/he rotates the array by rotating the scroll wheel by two positions clockwise, moving "6" to the position where "8" was located initially. At the moment the user starts rotation, the difference in 3D depth of the digits disappears for higher security. After rotation by an appropriate amount as shown in Figure 2(c), the user releases the finger from the display, which confirms that the user's choice is "6." Then, another rectangular array is displayed for the second digit as shown

(a) (b)

(c)

Figure 3: Digits with no position randomization. (a) Image for left eye. (b) Image for right eye. (c) Overlapped image.

(a) (b)

Figure 4: Implementation of 3DPIN (reproduction of Figure 2 in [8]). (a) Case wherein the camera sees blurred digits. (b) Case wherein the camera sees only one image.

in Figure 2(d). The completed stages are highlighted using black squares. If the user recognizes that a digit was input incorrectly, then s/he can revoke it by touching the "Back" button.

3. Implementation Details

We implemented 3DPIN on a smartphone equipped with the parallax barrier 3D display whose resolution is 800 × 480 pixels. The program was written in Java over Android 2.3.3. Figure 4 illustrates the proposed method at the moment when the 3D challenge shown in Figure 2(b) is given to the user. Figure 4(a) shows a photograph taken from the 3D spot right in front of the smartphone. The camera has only one lens, and we located this lens at the orthogonal point in front of the smartphone. Then, its view is slightly different from that of the left eye and that of the right eye. As a result, it only sees a blurred mixture of these two images. Figure 4(b) shows a photograph taken at a slight angle from the position of the left eye. We can see that the camera clearly captured the single image for the left eye.

We explain the realization of 3D effects in more detail. The smartphone that we used for the implementation allows us to express various levels of depth specified by an integer. If the depth is set as 0, it is located on the same plane of the LCD display, and the images for the left and right eyes are identical. On the other hand, a negative depth implies that the corresponding object is located at a deeper plane. This effect is realized by horizontally shifting an object for the left and right eyes to the left and right by an appropriate amount. The amount of shift is determined by the absolute value of the depth. The larger the absolute value, the more the object shifted. In contrast, to represent a positive depth, the object is shifted in the opposite direction.

Although various depth values may be assigned to each digit, we use only the numbers with fixed absolute values for a session. For example, we may assign +2 to the indicator digit and −2 to the other nine digits, or vice versa. The rationale for this assignment is related to the security and usability of the proposed method. First, we explain the security aspect. In Figure 4(a), we already observed that a one-lens camera may see a blurred image, which is caused by the horizontal shift that we explained in the previous paragraph. The shift of the indicator digit, that is, "8," should be done in the opposite direction from the other nine digits, because its depth has a different sign from that of the other digits. However, as shown in Figure 4(a), it is not easy to identify the image for either the left or the right eye from the blurred image. Therefore, it is not easy for a camera to find the indicator digit if all digits have the same absolute values in their depths. Our choice of depth is also justified from the viewpoint of usability. If all digits have distinct depths, a user may have difficulty discerning which one is the most prominent one or the deepest one. Moreover, the user has to know in advance whether the phantom indicator should be the most prominent one or the deepest one. By fixing the absolute values of depths, the user

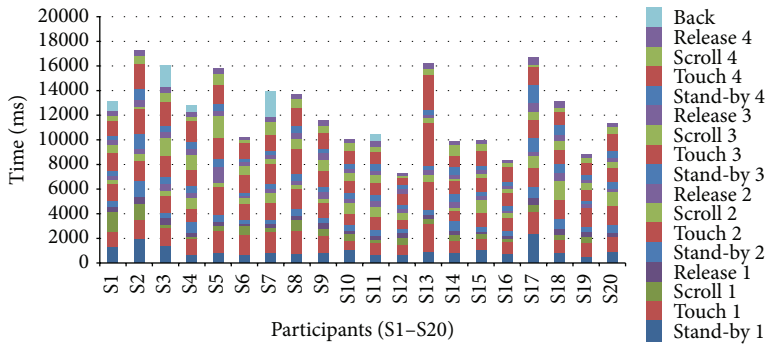

Figure 5: Distribution of authentication speed for 20 subjects (ms).

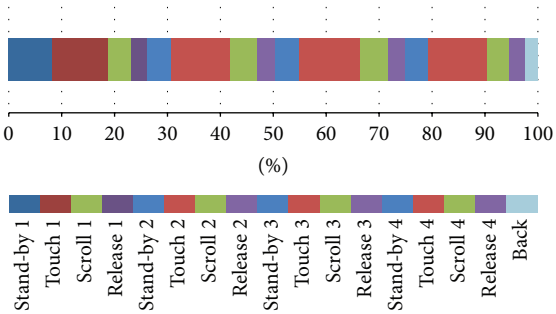

Figure 6: Tasks for an authentication session.

does not need to know this choice in advance, but s/he only has to find out the digit with a different depth from the other digits.

4. Performance Analysis

We conducted a usability study with twenty experimental subjects. Their ages ranged from 22 to 40 years, and six of the subjects were female. The purpose of this study was to analyze the rough performance of users and identify the bottleneck among various tasks comprising the authentication procedure for 3DPIN. At the beginning, the working mechanism of 3DPIN was explained in detail to each participant. Then, the participant was trained for 5 min to become accustomed to using 3DPIN and was guided to perform four authentication sessions. Two sessions were conducted using a fixed 4-digit PIN that the participant chose beforehand, and the other two sessions were conducted using randomly generated 4-digit PINs. When the participant failed to enter a correct PIN, s/he was asked to perform another session.

Now, we analyze the experimental results. Among the 80 sessions, 8 were failures and 8 more sessions were conducted. There was no failure in the retrial sessions. Therefore, the probability of erroneous input was 8/80 = 10.0%. Figure 5 shows the average time required for participants S1 to S20 to complete a session. Because we did not find any significant difference in the sessions using a fixed PIN and a random PIN, we did not distinguish between them in the graph. As a result, we obtained the median authentication time of 12.7 s with an average of 12.9 s and standard deviation of 2.9 s. Figure 5 also shows the tasks constituting an authentication session. That is, one stage to enter a single PIN digit is composed of four tasks, that is, *standby*, where the user gets ready to enter the next PIN digit; *touch*, where the user touches the scroll wheel and recognizes the phantom indicator; *scroll*, where the user scrolls the wheel so that the PIN digit is aligned with the phantom indicator; and *release*, where the user releases the finger after verifying the alignment. In addition, the user may perform one or more "*back*" tasks when s/he wants to cancel the incorrect input and redo the current stage.

Figure 6 shows the breakdown of times for these tasks, averaging all sessions of all participants. According to the measured data, the most time-consuming task is the "touch" task, where the participants try to identify the indicator digit by recognizing the difference in its 3D depth from the 3D depth of the other digits. It took about 1.38 seconds per stage. The participants also consumed nonnegligible time for the standby task in the first stage. We conjecture that this is because the users require some time to adjust themselves to execute the authentication application. The time for the "scroll" task in each stage is the sum of multiple movements. That is, a user has to rotate the digits by zero to five positions in an appropriate direction. However, the experimental results show that some participants failed to choose the optimal path in some stages. To be precise, nine among 320 stages had more than five movements. As a result, the average number of movements was 2.58, which is slightly greater than 2.5, the theoretically expected value. The total time required for the scroll task in each stage was 0.58 s on average.

We also had a short questionnaire session with each participant after the test. According to the survey data, 17

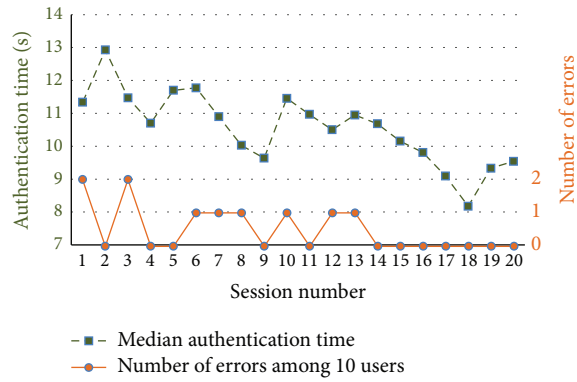

Figure 7: Change in median authentication time and error rate according to training.

Table 1: Comparison of PIN-entry methods for 4-digit PINs.

Method	Channel	Authentication time (s)	Error (%)	P_B	P_S
Regular PIN pad	—	<3	Approx. 0	1/10,000	Approx. 1.0
Undercover [11]	Haptic	32–45	>31.5	1/20,480	1/20,480
VibraPass [12]	Haptic	3.9–8.2	>14.8	1/10,000	1/70–1/5
Haptic Wheel [13]	Haptic	23.0	16.4	1/15,625	1/15,625
Phone Lock [9]	Haptic	28.2	10.4 (+5.6)	1/10,000	1/10,000
	Audio	12.2	4.8 (+6.9)	1/10,000	1/10,000
Spinlock [10]	Haptic	13.9–20.1	8.3 (+62.3)	<1/10,000	<1/10,000
	Audio	10.8–16.9	3.3 (+64.0)	<1/10,000	<1/10,000
3DPIN	3D	10.6	5.0	1/10,000	1/10,000

participants agreed that there should be a more secure PIN-entry method than the regular PIN pad, whereas the answers of 1 and 2 participants were negative and neutral, respectively. To the question asking whether they would use 3DPIN in daily life, 15 participants answered affirmatively, and 3 and 2 participants were negative and neutral, respectively. The reason for this encouraging result was that the participants felt very secure with 3DPIN. We asked whether they think that 3DPIN is more secure than the regular PIN pad and let them assign a score between 1 and 5 on the Likert scale. The average score was 4.25. However, they thought that 3DPIN was not as convenient as the regular PIN pad, giving a score of 2.05 on average to the question asking whether 3DPIN was more convenient.

Based on the results of the initial test, we designed another test. The purpose of this second test was to precisely analyze performance by using more session data. In addition, we tried to figure out the effect of training through repeated authentication sessions. It should be noted that the data in the initial test had been collected from participants who were not trained in 3DPIN. Then, the natural question is whether we may enhance the performance of the participants by training or not. Therefore, we formed a focus group of 10 volunteers from the 20 participants such that their average performance was approximately the same as the average of all participants. Then, each member of the focus group was guided to select his/her own PIN and perform an intensive experiment with 20 sessions with the fixed PIN. The dashed line shown in Figure 7 shows that the time required for a session gradually decreases, although there are a few exceptional values. For example, the median value among the 10 subjects was 9.5 s in the last session, and it temporarily dropped to even 8.2 s in the third-from-the-last session. The average over 20 sessions was 10.6 s. The solid line shown in Figure 7 shows that the error rate also decreases as the users get accustomed to the new method. For example, there is no erroneous input in the final seven sessions, whereas the error rate of 20 consecutive sessions is $10/(20 \times 10) = 5.0\%$ on average. Therefore, we may conjecture that the error rate will converge to zero after the users are sufficiently trained.

5. Comparison with Related Works

In this section, we compare the performance of 3DPIN with that of the previous secondary channel-based PIN-entry methods as well as the regular PIN pad. Table 1 summarizes the results. It lists various PIN-entry methods with the secondary channels that they use and shows the authentication time and error rate. For reference, we also compare the resistance against a brute force attack and a shoulder-surfing attack. The resistance against a brute force attack, denoted by P_B, represents the probability that the attacker may pass the authentication test by randomly guessing a PIN. The resistance against a shoulder-surfing attack, denoted by P_S, represents the attacker's success probability after observing one session.

As shown in Table 1, the proposed method guarantees much better performance than the previous methods. First,

Undercover [11] and Haptic Wheel [13] require a considerable amount of time for authentication and the rate of erroneous input is too high to be deployed in real-life applications. Although VibraPass [12] is almost as fast as the regular PIN pad in some settings (with a "low lie overhead" using the term defined by De Luca et al. [12]), its security is not significantly better than that of the regular PIN pad. That is, a shoulder-surfer can reduce the size of the candidate PIN set to as small as five after observing only one authentication session. Moreover, it suffers from a relatively high error rate (De Luca et al. [12] defined an error as the case where the user inputs incorrect values in three consecutive trials, which represents the common practice in ATMs. We recalculated the error rate according to our definition of error). Phone Lock [9] and Spinlock [10] have a novel feature that they may be used with two different channels, that is, either a haptic channel or an audio channel. In particular, the schemes with an audio interface guarantee competitive authentication time. However, it should be noted that it does not include the time for reset where a user cancels a PIN-entry process, but it only includes the successful case with no error and no reset. The figures in the parentheses in the "Error" column of Table 1 represent the reset rate. We see that Spinlock requires a reset task in more than half of the authentication trials. Therefore, the authentication time will be significantly greater if we take the time for the reset task into account. As explained in the previous section, our data for authentication time already include the time for touching the "back" button and reentering the current PIN.

We should also take into account other usability aspects. First, note that an earphone should be prepared for a secure audio channel, which significantly degrades the usability and further increases the authentication time if we include the time for the user to pick up an earphone and connect it to the device. In addition, most of the previous methods are not fully compatible with 4-digit PINs. For example, Spinlock [10] uses the combination of digits and directions as in a dial-based safe, and the PIN is written as, for example, "5 to the right, 3 to the left, 4 to the right, and 2 to the left." If we want to enter the PIN for our bank account on a banking application of a smartphone, there should be a compatible mapping between the regular PIN and the Spinlock PIN. Because this mapping is not straightforward, the user essentially has to memorize two different PINs, that is, the 4-digit PIN for ATM banking and the Spinlock PIN for smartphone banking. Note that this is not the case in 3DPIN.

In summary, the PIN-entry time, the error rate, and the other usability aspects of 3DPIN are very promising as compared to those of related works, and it is a practical solution for authentication. In addition, as verified in the training test in the previous section, its performance may be significantly improved as compared to the values given in Table 1.

Finally, we briefly mention other related works. The concept of using a sweet spot for security is not a completely new one but has already been suggested in the context of visual secret sharing [17]. In this scheme, the secret information can be recovered only at a sweet spot when the two transparent shares are located in parallel with an exact amount of space between them. However, this approach cannot be applied to authentication. A 3D visual channel was also used by Lee and Nam [18] as a secure interface, but their method did not fully utilize the advantage of the 3D channel and did not aim at achieving the maximum level of security. As a result, its P_S was 1/10, which was significantly higher than that of the proposed 3DPIN although it was ten times lower than that of the regular PIN pad. One may also consider an approach to physically obstruct the attacker's view. For example, a user may shield the device with his/her hand [19]. However, this method may leak some partial information about a PIN. There is also a method that uses a back-of-device panel [20], but this interface is not available in most current off-the-shelf smartphones. Finally, we remark that another kind of secure visual channel may be implemented if an additional device with short-range communication capability is available [21, 22].

6. Discussion on Interface Design

In this section, we explain the interface design of 3DPIN in more detail and discuss a few issues to improve its performance and usability. First, we would like to remark that the final layout of 3DPIN shown in Figure 2 is the result of our multiple-round pilot study. In our initial design stage, we have considered the following four factors:

(i) Arrangement of digits: we considered three alternatives: linear (see Figures 8(a) and 8(b)), diamond (see Figure 8(c)), circular, and rectangular (see Figure 2) arrangements.

(ii) Indicator types: we considered two alternatives. The first one was to use visible and explicit indicator symbols as in the traditional dial lock. For indicators, ten distinct graphic symbols such as a diamond (◆), a star (★), and a club (♣) were selected and each symbol was located next to each digit from 0 to 9 (see Figure 8(a)). In this version, which can be regarded as a 3D version of the method in [7], the 3D effect was given to the indicators instead of digits. The second alternative was not to use any indicator, which is the final design shown in Figure 2.

(iii) Interface for digit movement: in the initial prototype shown in Figure 8(a), the digits were moved by two buttons, "Left" and "Right," which required too many button touches. As an alternative, we adopted scrolling interface, that is, a linear scroll pad for the linear arrangement (see the pad with five sections in Figure 8(b)) and a scroll wheel for the diamond, circular, and rectangular arrangements (see Figure 8(c)).

(iv) Fonts of digits: line thickness, size, and shapes of PIN digits may affect the performance of PIN-entry.

To decide the best design in the aspect of authentication time and error rate, we tried various combinations of the above factors in an informal pilot study and finalized the current design, that is, a rectangular arrangement with a phantom indicator and a scroll wheel. As for the choice of

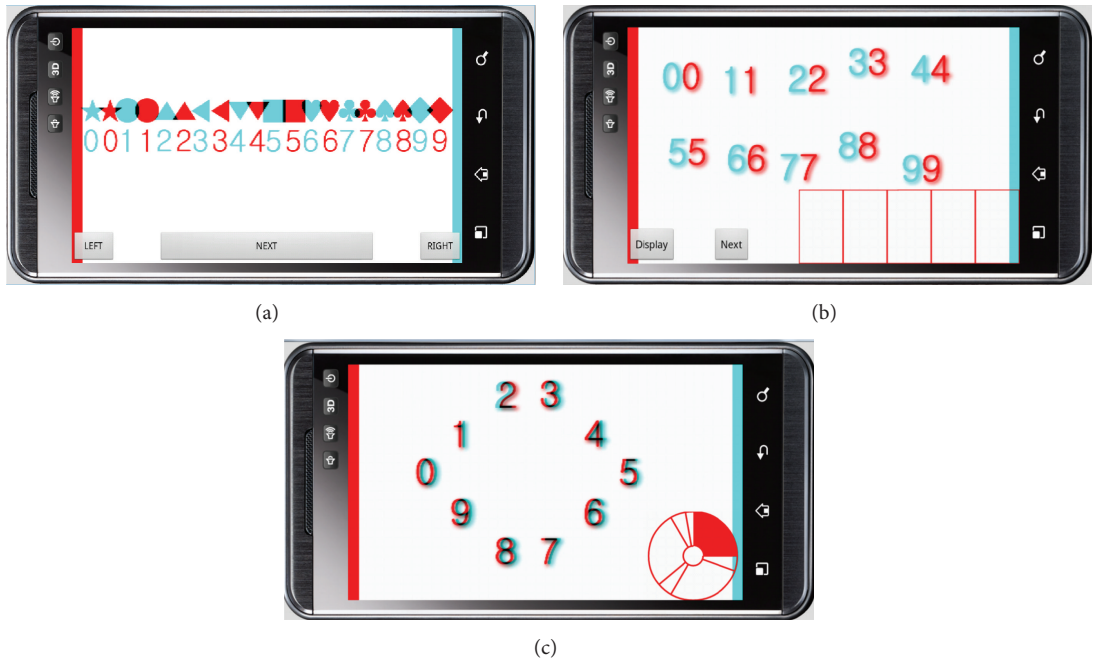

FIGURE 8: Alternative design of 3DPIN. (a) Linear arrangement, visible indicators (graphic symbols), and button interface for digit movement. (b) Linear arrangement, phantom indicator, and linear scroll pad. (c) Diamond arrangement, phantom indicator, and scroll wheel.

font, it was found out that a large and slim figure with a shadow effect was the best choice as shown in Figure 4.

However, we do not claim that the current design of 3DPIN is the optimal one. In the interview with the participants of our usability test, some participants raised questions about the layout of 3DPIN. The main issues were that the rectangular layout and the scroll wheel do not match each other intuitively and that sometimes participants tend to forget the position of the phantom indicator while rotating the digit array. This implies that, for better usability, qualitative aspects should be considered as well as quantitative aspects such as authentication time and error rate. In addition, the quantitative aspect itself could be improved. For example, according to the experimental results shown in Figure 6, the most time-consuming task is the "touch" task. Then, it would be promising to find an alternative design which focuses on reducing the bottleneck. For this purpose, a more thorough and in-depth adjustment and evaluation on user interface should be done. In addition, it would also be interesting to devise a tool to educate the users for better performance and verify the effectiveness of this tool by a more rigorous inspection, for example, by performing a regression analysis. We leave these issues as our future work.

7. Conclusion

In this paper, we proposed a PIN-entry method that uses the 3D display of a smartphone as the secure channel for data transmission. The proposed method, 3DPIN, guarantees fast authentication and low error rate by using an easy user interface and minimizing the amount of finger movement. However, there are still many open research issues to improve the usability of 3DPIN as mentioned in the previous section. In addition, it would be an interesting research direction to develop a 3D interface for entering a general password instead of a numeric PIN. Finally, the clear limit of 3DPIN is that it is restricted to devices with 3D displays. Therefore, the development of a unimodal PIN-entry method using only a standard visual channel would be promising.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by INHA University Research Grant. We would like to thank Jae Hyeong Lee and Hyeonjin Nam, for their help in the implementation and performance analysis, and all voluntary participants of our experiments.

References

[1] H.-M. Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958–961, 2000.

[2] J.-J. Shen, C.-W. Lin, and M.-S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414–416, 2003.

[3] S. Furnell, "An assessment of website password practices," *Computers and Security*, vol. 26, no. 7-8, pp. 445–451, 2007.

[4] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? The security of customer-chosen banking

PINs," in *Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers*, vol. 7397 of *Lecture Notes in Computer Science*, pp. 25–40, Springer, Berlin, Germany, 2012.

[5] J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," in *Proceedings of the 33rd IEEE Symposium on Security and Privacy (SP '12)*, pp. 538–552, San Francisco, Calif, USA, May 2012.

[6] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*, pp. 236–245, October 2004.

[7] M.-K. Lee, "Security notions and advanced method for human shoulder-surfing resistant PIN-entry," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 695–708, 2014.

[8] M.-K. Lee, J. B. Kim, and M. K. Franklin, "3DPIN: enhancing security with 3D display," in *Proceedings of the IEEE 3rd Global Conference on Consumer Electronics (GCCE '14)*, pp. 129–130, Tokyo, Japan, October 2014.

[9] A. Bianchi, I. Oakley, V. Kostakos, and D.-S. Kwon, "The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," in *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '11)*, pp. 197–200, ACM, 2011.

[10] A. Bianchi, I. Oakley, and D.-S. Kwon, "Spinlock: a singlecue haptic and audio PIN input technique for authentication," in *Haptic and Audio Interaction Design (HAID 2011)*, vol. 6851 of *Lecture Notes in Computer Science*, pp. 81–90, Springer, 2011.

[11] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: authentication usable in front of prying eyes," in *Proceedings of the 26th Annual CHI Conference on Human Factors in Computing Systems (CHI '08)*, pp. 183–192, ACM, April 2008.

[12] A. De Luca, E. von Zezschwitz, and H. Hußmann, "VibraPass: secure authentication based on shared lies," in *Proceedings of the Conference on Human Factors in Computing Systems (CHI '09)*, pp. 913–916, ACM, Boston, Mass, USA, April 2009.

[13] A. Bianchi, I. Oakley, J. K. Lee, and D. S. Kwon, "The haptic wheel: design & evaluation of a tactile password system," in *Proceedings of the 28th Annual CHI Conference on Human Factors in Computing Systems (CHI '10)*, pp. 3625–3630, ACM, Atlanta, Ga, USA, April 2010.

[14] A. Bianchi, I. Oakley, and D.-S. Kwon, "Open sesame: design guidelines for invisible passwords," *Computer*, vol. 45, no. 4, pp. 58–65, 2012.

[15] A. S. Seiderman and S. E. Marcus, *20/20 is Not Enough: The New World of Vision*, Knopf, 1990.

[16] F. June, *An Introduction to 3D Computer Graphics, Stereoscopic Image, and Animation in OpenGL and C/C++*, CreateSpace Independent Publishing Platform, 2nd edition, 2011.

[17] K. Kobara and H. Imai, "Limiting the visible space visual secret sharing schemes and their application to human identification," in *Advances in Cryptology—ASIACRYPT 96*, vol. 1163 of *Lecture Notes in Computer Science*, pp. 185–195, Springer, Berlin, Germany, 1996.

[18] M.-K. Lee and H. Nam, "Secure and fast PIN-entry method for 3D display," in *Proceedings of the 7th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '13)*, pp. 26–29, August 2013.

[19] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," in *Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security (SIGSAC '13)*, pp. 37–48, ACM, May 2013.

[20] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen et al., "Back-of-device authentication on smartphones," in *Proceedings of the 31st Annual CHI Conference on Human Factors in Computing Systems (CHI '13)*, pp. 2389–2398, ACM, Paris, France, May 2013.

[21] D. K. Yadav, B. Ionascu, S. V. K. Ongole, A. Roy, and N. Memon, "Design and analysis of shoulder surfing resistant PIN based authentication mechanisms on google glass," in *Financial Cryptography and Data Security*, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds., vol. 8976 of *Lecture Notes in Computer Science*, pp. 281–297, 2015.

[22] D. Zhang, D. Zhang, H. Xiong, C.-H. Hsu, and A. Vasilakos, "BASA: building mobile Ad-Hoc social networks on top of android," *IEEE Network*, vol. 28, no. 1, pp. 4–9, 2014.