논문 21-46-05-14

The Journal of Korean Institute of Communications and Information Sciences '21-05 Vol.46 No.05
https://doi.org/10.7840/kics.2021.46.5.890

시각장애인을 위한 개인식별번호 입력 기술

전일수[•], 유제니오[*], 김명식[**], 임완수[°]

An Assistive PIN Input Technology for the Visually Impaired

Il-Soo Jeon[•], Manuel Eugenio Morocho-Cayamcela[*], Myung-Sik, Kim[**], Wansu Lim[°]

요약

개인 식별 번호(PIN)는 시각 장애인이 자동 입출금기(ATM), 디지털 도어록, 휴대폰과 같은 디지털 장치에 접근하기 위해 선호되는 인증 방법이다. 최신 PIN 입력 기술은 훔쳐보기, 화면 녹화와 스머지 공격을 통한 보안 침해에 취약한 것으로 조사되었다. 이에, 본 논문은 사용자의 개인정보를 강화하고 반복적인 터치 동작을 개선하여 강화된 PIN 입력 기술을 구현한다. 제안한 PIN 입력 기술은 이전 기술과 비교하여 더 효율적이고 쉬운 인증이 가능하도록 하였으며, 안드로이드 모바일 장치에 구현하였다. 실험 결과 일련의 무작위 가청 키를 활용한 제안한 PIN 입력 기술이 시각 장애인 같은 보안 취약계층에 대한 개인정보 침해에 대응할 수 있는 것으로 나타났다. 구체적으로 IESPIT 인증의 성공률은 91.5%로 이전 모델보다 13% 더 향상하였고, 인증 속도와 사용 편의성을 위한 t-검정 결과는 IESPIT의 평균 점수가 1% 수준에서 이전 버전보다 통계적으로 유의미했음을 보여주었다.

키워드 : 보조 입력 기술, 입력 장치와 전략, 보안, 사회 문제, 시각장애인

Key Words : Assistive technologies, input devices and strategies, security education, social issues, visually impaired people.

ABSTRACT

Personal identification number (PIN) passwords are the preferred authentication method for visually impaired users to access digital devices like automated teller machines (ATMs), digital door locks, and cellular phones. The latest PIN input techniques have shown vulnerability to security breaches via shoulder-surfing, screen recording, and smudge attacks. In this paper, we propose the Improved Enhanced Simple PIN Input Technique (IESPIT), an improved PIN input technique that reinforces privacy of the user and eliminates the need for repeated touch actions, thereby making it an efficient and easier verification technique as compared to its predecessors. We implemented the concept on an Android mobile device and conducted experiments to verify the feasibility of our scheme. Results indicate that our proposed methodology can counter the most popular privacy assaults to this vulnerable population by utilizing a set of randomized audible keys. Tests on 10 volunteers demonstrated that the authentication with IESPIT was 13% faster than its closest predecessor, with a success ratio of 91.5%. A t-test for the equality of means among the participants' perception of authentication speed, convenience, and ease of use further evinced shows that the mean scores of IESPIT were statistically significant from the previous version at the 1% level.

※ 본 연구는 금오공과대학교 교수연구년제에 의하여 연구된 실적물입니다.

[•] First Author : Kumoh National Institute of Technology, Department of Electronic Engineering, isjeon@kumoh.ac.kr, 정회원

[°] Corresponding Author : Kumoh National Institute of Technology, Department of Aeronautics, Mechanical and Electronic Convergence Engineering, wansu.lim@kumoh.ac.kr, 정회원

[*] Yachay Tech University, School of Mathematical and Computational Sciences, 학생회원

[**] Kumoh National Institute of Technology, Department of Electronic Engineering

논문번호 : 202012-335-D-RN, Received December 29, 2020; Revised February 22, 2021; Accepted February 22, 2021

Ⅰ. Introduction

Nowadays, people heavily rely on passwords and other verification protocols to access their personal and public digital devices[1-3]. To this effect, PINs have been utilized for a long time to validate users into their systems[4-8]. A PIN is a four-digit key that authenticates users into ATMs, swiping credit cards, and unlocking digital door locks[9-11]. Despite the existence of bio-metric verification systems, such as fingerprint, iris, and face recognition, PINs are widely popular among visually impaired individuals as they are easy to memorize, convinient, and trustworthy[12-14]. In addition to that, PINs provide a more robust verification system as the bio-metric verification systems are vulnerable to subversion[12, 13]. As discussed in [12] and [13], fingerprint, iris, and face recognition-based verification systems can be intruded easily by obtaining the fingerprint and facial photograph of an individual. Consequently, developing an easy, robust, and secure PIN input mechanism for such users is an important domain of research[15].

Visually impaired users are vulnerable to security breaches such as shoulder-surfing, screen recording, and smudge attacks. Shoulder-surfing attacks occur when the attacker looks over the victim's shoulder to obtain their password or PIN[16]; screen recording captures the victim's phone screen without their knowledge or consent[17], and a smudge attack discerns the password pattern of a touchscreen device by examining the oily smudges left behind by the user's fingers when unlocking their device[18]. Thus, secure PIN input techniques[19-31] have been extensively studied. To resist these attacks, researchers have used non-visual channels, such as sound and/or vibrations[25-32], as feedback which have proved to be very purposeful approaches[33]. [34] proposed The Phone Lock, an auditory and haptic PIN input method for mobile devices resistant to shoulder-surfing attacks. Their technique is engineered for vulnerable groups, such as children, elders, individuals with cognitive disabilities, etc., and has emerged as one of the most feasible PIN input techniques.

Here, we propose Improved Enhanced Simple PIN Input Technique (IESPIT), an assistive PIN input application designed to be intuitive, with no visible information on the touchscreen, and more efficient than earlier technologies, as it eliminates the need of recurrent haptic feedback from the user to interact with the audible keys to enter the PIN. Unlike its predecessors, the IESPIT method introduces the speaking interval and response time variables to reduce the error ratio of the PIN input as well as time taken to complete authorization. Furthermore, we compare the authentication accuracy and speed of this technique with its nemesis, the Enhanced Simple PIN Input Technique (ESPIT). We implemented the application on a mobile phone running on Android operating system to evaluate the feasibility of the scheme for the visually impaired. Results demonstrate that IESPIT is the faster and more practical PIN input technique.

Ⅱ. Related Work

In this section, we investigate pertinent mobile authentication techniques for the visually impaired. With this demographic now predominantly using touchscreen devices, new security challenges have arisen[10,38-40]. As per the norm, to protect smartphones from unauthorized access (and, consequently, the personal information stored in them), users need to validate their identity through user authentication methods[41,42]. Our work focuses on conducting user validations with assistive PIN inputs.

[35] introduced *PinPad*, a multi-touch touchpad that can be used to enter PIN numbers. The interface comprises an array of 40×25 tactile sensors and a braille module for data input. However, when the user enters the PIN with multi-touch gestures, such as two-finger scrolling and pinching, the system becomes susceptible to shoulder-surfing attacks.

The *Phone Lock* system is a touch screen PIN input method that obtains sound cues from a user's earphones[26]. The system interface displays 10 targets on the touchscreen, with each target mapped to a random sound cue from 0 to 9. Although each target corresponds to a randomized sound cue, the numbers mapped to targets follow a sequential order. When a target is touched, and a number from the sound cue a digit of the PIN, the user drags the target to a center circle and removes their finger from the screen to complete entering one digit of the PIN. If the sound cue does not match the digit of the PIN, the user has to move to another target and repeat the process until the right number is sought. A major limitation of this work, for a visually impaired individual, is the encumbrance of locating the precise position of the targets as well as the center circle in the user interface (UI) without visual feedback, thereby facilitating an increased number of failed authentication attempts.

[36] proposed Simple PIN Input Technique (SPIT), whereby a user interacts with a mobile device via sound cues that is relatively easier to use than The Phone Lock. SPIT overcomes the problems encountered in The Phone Lock by employing a single large-squared target at the center of the screen to procure each digit of the PIN, as seen in Fig. 1. The mapped sound cues are randomized before entering a digit of the PIN[36]. SPIT also uses sound cues to authenticate the user, each one corresponding to a PIN digit from 0 to 9. When the user touches the target to enter a PIN digit, the system reproduces a sound cue from a randomly ordered list through the user's earphone. When the user hears a sound cue that matches a digit of the PIN to be entered, they swipe from left to right on the target to enter the corresponding PIN digit. Thereafter, this ordered list is reconfigured in the system before receiving input from the next PIN digit[37]. In Fig 1, the four small boxes correspond to the digits of the PIN. Fig 1(a) shows the initial screen of SPIT waiting for the user to input the first digit, and Fig 1(b) represents the screen where the second digit is to be entered. The empty red circle within the box implies that the corresponding digit has to be entered, while the filled circle denotes that the corresponding digit has been entered. Three buttons are deployed at the bottom viz., the "OK" button to validate the PIN once all digits have been entered; "BACK" button to delete the last digit entered; and "CANCEL" button to delete all digits entered[37]. Although SPIT is intuitive as a PIN input method and resistant to security attacks, it still harnesses visible information like rectangles, circles, and buttons. Locating these buttons on the screen can be tedious for a visually impaired user, limiting the practicality of the scheme. Moreover, such a user may tend to misplace the digit indices in the middle of the process, given that SPIT necessitates haptic feedback multiple times to enter a single digit.

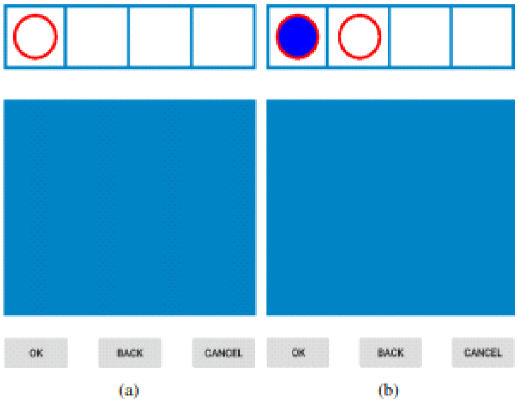


Fig. 1. SPIT UI (a)Initial screen ready to receive the first digit of the PIN (left);(b) Wait screen for entering the second digit (right).

In 2017, [37] proposed ESPIT (Enhanced Simple PIN Input Technique), which uses objects instead of numerals as constituents of the PIN. ESPIT addresses the shortcomings of SPIT by creating a PIN with four different objects instead of a four-digit number. These objects are characterized into numbers, colors, fruits, and a body parts. Each instance of a PIN object is chosen from a total of 10 instances of objects derived from the lexicon enumerated. ESPIT was developed specifically for children, the elderly and visually impaired populace. An advantage of this method is that the order of input among objects constituting the PIN is independent, and the UI is designed with only one touching target on the screen. Like SPIT, ESPIT generates a randomized ordered list for each of the 10 instances of the objects. When a user touches the screen, the system generates a sound corresponding

Table 1. Summary of related works on PIN input technologies for visually impaired.

Application	Proposal	Interface	Limitations	Reference
PinPad	A multi-touch touchpad that can be used to enter PIN numbers.	An array of 40×25 tactile sensors and a braille module for data input.	User needs to enter the PIN with multi-touch gestures, such as two-finger scrolling and pinching, leaving the system vulnerable to shoulder-surfing attacks.	[35]
The Phone Lock	It employs targets on the screen of a mobile application.	10 touching targets on the touch-screen mapped to random sound cues from 0 to 9. The user gets audible feedback via earphones	Tedious for a user with restricted vision to locate precise position of the targets and center circle in the UI without visual feedback. The numbers mapped to the targets must be in sequential order.	[26]
SPIT	It randomizes the mapped sound cues before each digit of the PIN is entered.	Single large-squared target at the center of the screen to acquire each digit of the PIN. User gets audible cues via earphones.	Utilizes visible information, such as rectangles, circles, and buttons, which make it susceptible to over-the-shoulder attacks. Also, cumbersome to locate these buttons on the screen for a visually impaired user.	[36]
ESPIT	Addresses the weakness of SPIT by harnessing 10 instances of an object instead of an integer as the constituent of a PIN.	One touching target on the touch-screen. When the space is touched, system generates a sound associated with one of the instances to the user via earphones.	The user needs to touch the screen repeatedly to play sound cues and enter one instance of the PIN. In reality, this may introduce errors during the PIN input.	[37]
IESPIT	Uses four objects viz., number, color, fruit, and body part, and 10 different object-instances instead on numbers as PIN constituents. It replaces the need for repeatedly touching the screen to hear a sound clue, by automatically reproducing the instances when the application boots or resets. It defines two novel variables viz., *speaking interval*, and *response time* to reduce the error ratio and speed of authentication.	The entire screen acts as a target to receive touch and swipe actions from the user upon hearing audible cues via earphones.	While it can be effectively used in isolation as a PIN input technique for the visually impaired, it can be further enhanced with two-factor authentication methods such as, face recognition, fingerprint recognition, etc.	–

to one of the object instances to the user via their earphones. If this sound resembles that of an instance registered in the password, then they swipe from left to right to confirm the instance as a constituent of the PIN. Table 1 provides the summary of elated works on PIN input technologies for visually impaired.

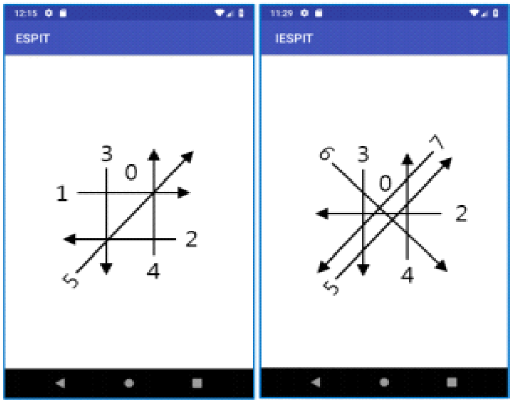
Ⅲ. Proposed PIN Input Technique: IESPIT

In this section, we elaborate on our proposed PIN input technique called IESPIT, which is an improved version of the ESPIT. Considering that we focus exclusively on enhancing the PIN input method proposed in [37], and that our proposed authentication method is built upon ESPIT, we have assumed that the additional security processes, such as registration, PIN hashing and blacklisting, tunnel encryption, etc. are established sub-processes. We describe the implementation of both, ESPIT and IESPIT on a mobile device for a visually impaired user. The user interfaces of both applications are similar and devoid of visible components on the touchscreen like buttons and text boxes. The entire screen is configured as a target, set to receive touch and swipe actions from the user.

The proposed scheme was designed to improve the ESPIT, which required repeated tactile feedback to enter a single constituent of the PIN. In reality, we discover that some users touch the screen by inertia, introducing errors in the PIN input phase. Table 2 shows the four objects (i.e., number, color, fruit, and body part), along with their respective instances. We replaced the need for haptic feedback each time a user wanted to hear an instance, by automatically producing the sound cues when the application was booted or reset. Instead, when the user heard a registered instance, they only touched the screen to confirm it as a constituent of the PIN.

Table 2. The 10 instances of each object used as authentication keys.

Number	Color	Fruit	Body Part
0	White	Apple	Head
1	Black	Orange	Eye
2	Grey	Banana	Nose
3	Red	Grape	Mouth
4	Green	Peach	Ear
5	Blue	Pear	Neck
6	Yellow	Strawberry	Hand
7	Brown	Tomato	Foot
8	Purple	Mango	Arm
9	Pink	Melon	Leg



(a) ESPIT (b) IESPIT

Fig. 2. Illustration of swipe actions directions in (a)ESPIT UI (left) and (b)proposed IESPIT UI (right).

Fig. 2 illustrates the direction of the configured swipe actions in both applications, represented by numbered arrows.

The role of each swipe action in Fig. 2 is described in detail in Table 3. Please note that only action “0” was undefined in both cases, as it indicated a touch action and invoke different reactions viz., in ESPIT to trigger the audible cues, and, in IESPIT, to confirm an object instance. Additionally, swipe action “1” in IESPIT was undefined to avoid confusion with its ESPIT counterpart, which confirmed an object instance. Actions “2” to “5” were identical in both methods and defined the procedures of correction, restart, exit, and setting a new PIN, respectively. Actions “6” and “7” (undefined in ESPIT) in IESPIT were programmed to automatically increase and decrease, respectively, the speed of spoken instances, i.e., the speaking interval, a custom variable defined as the time elapsed between the start of an audible cue and beginning of the next one.

The IESPIT interface allowed the user to adjust this interval according to their own response abilities. We also introduced a response time variable, defined as the minimum time required to detect a touch action from the beginning of an audible cue. We measured these values by conducting experiments with 10 volunteers multiple times to minimize authentication failure. After the initial calibration, we configured the response time to 0.5 seconds, which means that if a touching action is detected within 0.5 seconds of playing an audible instance, it is considered as an input from the previous instances.

Fig. 3 exemplifies how different touch actions in the same speaking intervals were detected as different instances in IESPIT. Touch action “A” was recognized as a confirmation for the first instance, as the action is performed within the response time, while touch action “B” corresponded to the second instance. A response time variable was established

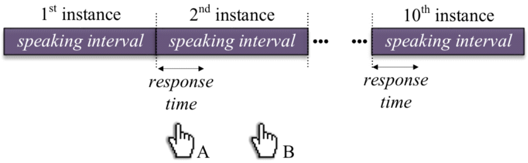
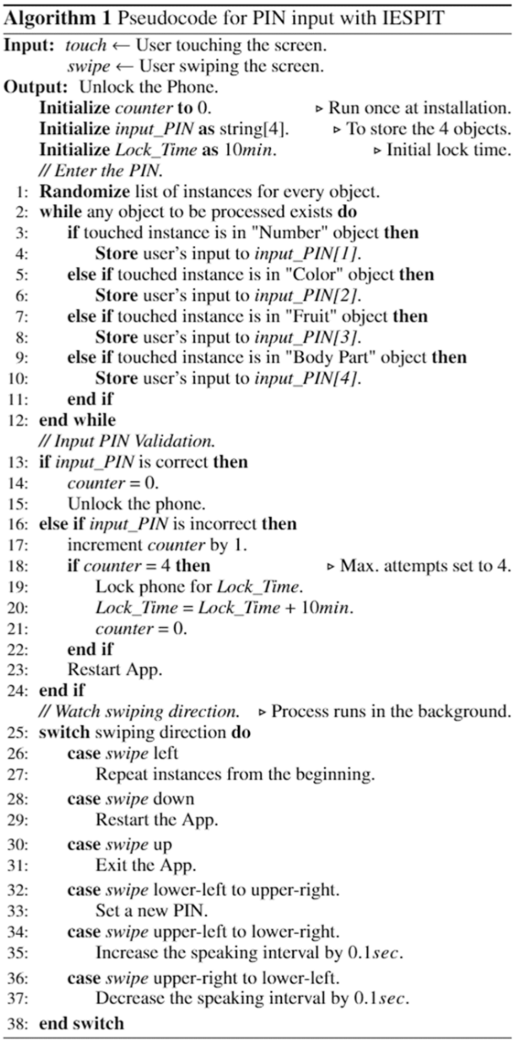


Fig. 3. Illustration of IESPIT timeline.

Table 3. Role of each directed swipe for ESPIT and IESPIT.

Swiping		ESPIT	IESPIT
Number	Direction		
0	-	To trigger the spoken instances.	**To confirm the instance when the user hears it.**
1	From left to right.	**To confirm the instance when the user hears it.**	-
2	From right to left.	To repeat the spoken instances from the beginning (for the current object).	To repeat the spoken instances from the beginning (for the current object).
3	From top to bottom.	To restart the app.	To restart the app.
4	From bottom to top.	To exit the app.	To exit the app.
5	From lower left to upper right.	To set a new PIN	To set a new PIN.
6	From upper left to lower right.	-	To increase the speaking interval by 0.1 seconds.
7	From upper right to lower left.	-	To decrease the speaking interval by 0.1 seconds.



```
Algorithm 1 Pseudocode for PIN input with IESPIT
Input:  touch ← User touching the screen.
        swipe ← User swiping the screen.
Output: Unlock the Phone.
    Initialize counter to 0.                    ▷ Run once at installation.
    Initialize input_PIN as string[4].          ▷ To store the 4 objects.
    Initialize Lock_Time as 10min.              ▷ Initial lock time.
    // Enter the PIN.
    Randomize list of instances for every object.
    while any object to be processed exists do
        if touched instance is in "Number" object then
            Store user's input to input_PIN[1].
        else if touched instance is in "Color" object then
            Store user's input to input_PIN[2].
        else if touched instance is in "Fruit" object then
            Store user's input to input_PIN[3].
        else if touched instance is in "Body Part" object then
            Store user's input to input_PIN[4].
        end if
    end while
    // Input PIN Validation.
    if input_PIN is correct then
        counter = 0.
        Unlock the phone.
    else if input_PIN is incorrect then
        increment counter by 1.
        if counter = 4 then                     ▷ Max. attempts set to 4.
            Lock phone for Lock_Time.
            Lock_Time = Lock_Time + 10min.
            counter = 0.
        end if
        Restart App.
    end if
    // Watch swiping direction.                 ▷ Process runs in the background.
    switch swiping direction do
        case swipe left
            Repeat instances from the beginning.
        case swipe down
            Restart the App.
        case swipe up
            Exit the App.
        case swipe lower-left to upper-right.
            Set a new PIN.
        case swipe upper-left to lower-right.
            Increase the speaking interval by 0.1sec.
        case swipe upper-right to lower-left.
            Decrease the speaking interval by 0.1sec.
    end switch
```

Fig. 4. Pseudocode for PIN input with IESPIT.

in IESPIT to extend the actual speaking interval up to 0.5 seconds, which helped reduce not only the error ratio of a PIN input but also the time to complete authorization. The pseudocode of IESPIT can be found in Fig. 4.

Ⅳ. Security Analysis and Performance Evaluation

We performed a comparative study between the ESPIT and IESPIT techniques by installing the respective applications in an Android mobile phone. As they both have harbored no visible information on the UI and only harnessed a sound channel, we believe them to be resistant to the security attacks described in section I. Moreover, considering that the number of sound cues required to enter an instance was randomly chosen between 1 to 10, its guessing probability was computed as (1/10) for each object. Therefore, this probability of a PIN with four objects equaled $(1/10)^4$ per object. The proposed methodology can be easily extended to enhance the PIN security for guessing attacks by adding more categories of objects. Although in both methods, the PIN length is fixed, the security can be reinforced by simply adding more instances of each object.

We conducted a survey to evaluate whether the proposed IESPIT outperformed the ESPIT for authenticating visually impaired users into their digital devices. Fig. 5 shows volunteers performing authentication test for the IESPIT application. Fifty individuals participated in the test and completed a survey later on their experiences with both

Fig. 5. Volunteers in the performance and feasibility evaluations of both, ESPIT and IESPIT mobile applications.

Table 4. Quantitiative performance results of both methods.

ESPIT		IESPIT	
Success Ratio	Elapsed Time	Success Ratio	Elapsed Time
90.5%	27.5 *Sec*	91.5 %	24.4 *Sec*

Table 6. T-test results for ESPIT vs. IESPIT variables based on experiments and questionnaire.

Variable	ESPIT	IESPIT	Mean difference	t-value
Perceived Speed	0.473	0.542	-0.069	-8.915***
Convenience	0.329	0.377	-0.048	-7.475***
Ease of Use	0.114	0.165	-0.021	-4.421***

methodologies. Table 4 collates the results of the quantitative performance of both applications. The participants were trained for 5 min to: a) get acclimatized to the applications; and b) define an optimal speaking interval for the instances in IESPIT, which was determined, for this study, as 0.8-1.2 seconds based on personal response abilities.

Therefore, the actual speaking interval, for this study, was configured between 1.3-1.7 seconds, including the response time. Each participant performed the authentication 10 times for each method. Table 4 shows the averages from these trials. The elapsed time of verification for ESPIT and IESPIT was 27.5 and 24.4 seconds respectively. Thus, verification with IESPIT was 13% faster than with ESPIT. The success ratio i.e., the authorization success ratio for all attempted PIN input validation, was over 90% for both methods, with IESPIT peaking at 91.5%. Overall, we empirically proved that our proposed method outperformed the ESPIT in terms of the authentication speed.

Table 5 highlights the survey results of the qualitative performance of the two methods. User satisfaction for IESPIT surpassed its competitor. The participants believed that an object-based PIN was easier to memorize than a numeric PIN. All participants expressed their preference of using the ESPIT and IESPIT authentication methods to tackle dubious security attacks given the choice, and approved both applications for their user-friendliness. Resultantly, we conclude that IESPIT is a fast, easy-to-use, effective, and practical PIN input method for the visually impaired. We also envisage its benefits for the non-visually impaired where safeguarding from security attacks is concerned.

We performed a t-test on the data acquired from the survey to assess the differences in mean scores between ESPIT and IESPIT. The test proves statistical significance at the 1% level between variables, such as perceived speed, convenience, and ease of use; in the authentication experiment and survey. The statistical values are highlighted in Table 6. Regarding the statistical characteristics of this study, among the participants who tested the mobile application and filled the questionnaire, 52% were men and 48% were women. Their percentage ages were distributed as follows: 44% between the ages 26-35; 26% between the ages 36-45; 14% between the ages 18-25; 10% between the ages 46-55; and 6% older than 56.

Ⅴ. Conclusions

We proposed and implemented a practical, fast, effective, and easy-to-use assistive PIN input technique IESPIT, an improved version of the ESPIT method. To test the feasibility of implementing the proposed method, we performed multiple tests, by way of a comparative study, with 10 volunteers to measure the authorization speed and success rate.

Additionally, we conducted a survey on the volunteers to evaluate the user-friendliness of both

Table 5. Survey results for user satisfaction.

Questions	Responses		
	Yes	No	Similar
1. Do you think IESPIT is more convenient to use than ESPIT?	70%	10%	20%
2. Do you think that an object-based PIN is easier to memorize than a number-based PIN?	80%	5%	15%
3. If ESPIT/IESPIT were available as an authentication option in your phone, ATM, or a digital door lock. Will you use them if you feel that you are under a security attack?	100%	0%	
4. Do you think that it was difficult to use ESPIT/IESPIT as an authentication process?	0%	100%	

applications. Results indicate that verification with IESPIT was 13% faster than with ESPIT. The success ratio of both applications exceeded 90% with IESPIT edging its competitor by 1.5%. We envision this technique to also help bolster the overall security of digital devices, such as ATMs, digital door locks, and mobile phones, for the non-visually impaired demographic, despite taking longer to enter the PIN. Finally, while IESPIT can be used in isolation as an effective PIN input technique for the visually impaired, it can be further developed to support two-factor authentication methods like face recognition, fingerprint recognition, etc.

References

[1] S. Sim, et al., "Threat analysis of the smart doorlock systems using threat modeling," *J. KICS*, vol. 45, no. 11, pp. 1868-1877, 2020.

[2] K. Lee, et al., "Wireless-powered secure relaying protocols for minimizing secrecy outage probability," *J. KICS*, vol. 45, no. 7, pp. 1145-1157, 2020.

[3] K. Lee, et al., "Wireless-powered secure relaying protocols for minimizing secrecy outage probability," *J. KICS*, vol. 45, no. 7, pp. 1145-1157, 2020.

[4] M. Dascalu, A. Moldoveanu, O. Balan, R. G. Lupu, F. Ungureanu, and S. Caraiman, "Usability assessment of assistive technology for blind and visually impaired," in 2*017 E-Health and Bioengineering*, pp. 523-526, Jun. 2017.

[5] M. Sreelakshmi and T. Subash, "Haptic technology: A comprehensive review on its applications and future prospects," *Materials Today: Proc.*, vol. 4, no. 2, Part B, pp. 4182-4187, 2017.

[6] S. K. Card, A. Newell, and T. P. Moran, *The Psychology of Human-Computer Interaction*, Hillsdale, NJ, USA: L. Erlbaum Associates Inc., 1983.

[7] M. Lee, "Security notions and advanced method for human shoulder-surfing resistant pin-entry," *IEEE Trans. Inf. Forensics and Secur.*, vol. 9, no. 4, pp. 695-708, Apr. 2014.

[8] T. Kwon and J. Hong, "Analysis and improvement of a pin-entry method resilient to shoulder-surfing and recording attacks," *IEEE Trans. Inf. Forensics and Secur.*, vol. 10, no. 2, pp. 278-292, Feb. 2015.

[9] R. Kuber and S. Sharma, "Toward tactile authentication for blind users," *ASSETS '10*, in *Proc. 12th Int. ACM SIGACCESS Conf. Comput. and Accessibility,* pp. 289-290, NY, USA, 2010.

[10] S. Azenkot, K. Rector, R. Ladner, and J. Wobbrock, "Passchords: Secure multi-touch authentication for blind people," *ASSETS '12; in Proc. 14th Int. ACM SIGACCESS Conf. Comput. and Accessibility*, pp. 159-166, NY, USA, 2012.

[11] K. Helkala, "Disabilities and authentication methods: Usability and security," in *2012 Seventh Int. Conf. Availability, Reliability and Secur.*, pp. 327-334, Aug. 2012.

[12] M. Ali, A. Baloch, A. Waheed, M. Zareei, R. Manzoor, and F. Alanazi, "A simple and secure reformation-based password scheme," *IEEE Access*, vol. 9, pp. 11655-11674, Jan. 2021.

[13] S. W. A. Shah, A. Shaghaghi, S. S. Kanhere, J. Zhang, A. Anwar, and R. Doss, "Echo-ID: Smart user identification leveraging inaudible sound signals," *IEEE Access*, vol. 8, pp. 194508-194522, Oct. 2020.

[14] N. Wakabayashi, M. Kuriyama, and A. Kanai, "Personal authentication method against shoulder-surfing attacks for smartphone," in *2017 IEEE ICCE*, pp. 153-155, Jan. 2017.

[15] G. M. S. Silva, R. M. de C. Andrade, and T. de Gois R. Darin, "Design and evaluation of mobile applications for people with visual impairments: A compilation of usable accessibility guidelines," *IHC'19; in Proc. 18th Brazilian Symp. Human Factors in Computing Syst.*, pp. 1-10, NY, USA, 2019.

[16] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human

adversaries are more powerful than expected," *IEEE Trans. Syst., Man, and Cybernetics: Syst.*, vol. 44, no. 6, pp. 716-727, Jun. 2014.

[17] D. Shukla and V. V. Phoha, "Stealing passwords by observing hands movement," *IEEE Trans. Inf. Forensics and Secur.*, vol. 14, no. 12, pp. 3086-3101, Dec. 2019.

[18] M. D. Amruth and K. Praveen, "Android smudge attack prevention techniques," in *Intell. Syst. Technol. and Appl.*, pp. 23-31, 2016.

[19] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: Authentication usable in front of prying eyes," in *Proc. CHI*, pp. 183-192, 2008.

[20] A. D. Luca, E. von Zezschwitz, and H. Husmann, "Vibrapass: Secure authentication based on shared lies," in *Proc. CHI*, pp. 913-916, 2009.

[21] M. C. T. Perkovic and N. Rakic, "Sssl: Shoulder surfing safe login," in *Proc. Int. Conf. Softw., Telecommun. Comput. Netw.*, pp. 270-275, 2009.

[22] A. Bianchi, I. Oakley, J. K. Lee, and D.-S. Kwon, "The haptic wheel: Design & evaluation of a tactile password system," in *Proc. CHI*, pp. 3625-3630, 2010.

[23] I. O. A. Bianchi and D.-S. Kwon, "The secure haptic keypad: A tactile password system," in *Proc. CHI*, pp. 1089-1092, 2010.

[24] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," *WOOT '10; in Proc. 4th USENIX Conf. Offensive Technol.*, pp. 1-7, Aug. 2010.

[25] E. von Zezschwitz, A. Koslow, A. D. Luca, and H. Hussmann, "Making graphic-based authentication secure against smudge attacks," in *Proc. IUI*, pp. 277-286, 2013.

[26] T. Kwon and S. Na, "Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems," *Comput. & Secur.*, vol. 42, pp. 37-150, 2014.

[27] M.-K. Lee, "Security notions and advanced method for human shoulder-surfing resistant pin-entry," *IEEE Trans. Inf. Forensics and Secur.*, vol. 9, no. 6, pp. 695-708, 2014.

[28] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in *Proc. SOUPS*, pp. 13-19, 2007.

[29] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," *CHI'10; in Proc. SIGCHI Conf. Human Factors in Comput. Syst.*, pp. 1107-1110, Apr. 2010.

[30] J. Thorpe, P. van Oorschot, and A. Somayaji, "Pass-thoughts: Authentication with our minds," in *Proc. NSPW*, pp. 45-56, 2005.

[31] M. K. Lee, "A user interface for secure personal identification number input," *J. KIISC*, vol. 24, no. 3, pp. 27-35, 2014.

[32] A. Bianchi, I. Oakley, and D.-S. Kwon, "Spinlock: A single-cue haptic and audio PIN input technique for authentication," *HAID 2011: Haptic and Audio Interaction Design*, pp. 81-90, 2011.

[33] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, "Loud and clear: Human-verifiable authentication based on audio," in *26th IEEE ICDCS'06*, Lisboa, Portugal, Jul. 2006.

[34] 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 *Proc. TEI*, pp. 197-200, 2011.

[35] J. Jung, E. Youn, and G. Lee, "Pinpad: Touchpad interaction with fast and high-resolution tactile output," *CHI '17; in Proc. 2017 CHI Conf. Human Factors in Comput. Syst.*, pp. 2416-2425, NY, USA, 2017.

[36] I.-S. Jeon and E.-J. Yoon, "A simple pin input technique resisting shoulder surfing and smudge attacks," *Contemporary Eng. Sci.*, vol. 8, no. 17, pp. 747-755, 2015.

[37] I.-S. Jeon and M.-S. Kim, "An enhanced simple pin input technique resisting shoulder

surfing and smudge attacks," *Contemporary Eng. Sci.*, vol. 10, no. 5, pp. 203-210, 2017.

[38] B. Dosono, J. Hayes, and Y. Wang, ""i'm stuck!": A contextual inquiry of people with visual impairments in authentication," in *SOUPS 2015*, pp. 151-168, Jul. 2015.

[39] K. Fuglerud and O. Dale, "Secure and inclusive authentication with a talking mobile one-time-password client," *IEEE Secur. Privacy*, vol. 9, no. 2, pp. 27-34, Mar. 2011.

[40] S. A. Kleynhans and I. Fourie, "Ensuring accessibility of electronic information resources for visually impaired people: The need to clarify concepts such as visually impaired," *Library Hi Tech.*, vol. 32, no. 2, Jun. 2014.

[41] D. Briotto Faustino and A. Girouard, "Understanding authentication method use on mobile devices by people with vision impairment," *ASSETS '18; in Proc. 20th Int. ACM SIGACCESS Conf. Comput. and Accessibility*, pp. 217-228, NY, USA, 2018.

[42] D. Marques, L. Carriço, and T. J. V. Guerreiro, "Assessing inconspicuous smartphone authentication for blind people," *CoRR*, vol. abs/1506.00930, 2015.

전 일 수 (Il-Soo Jeon)
1995년 2월 : 경북대학교 전자공학과 박사
2004년 3월~현재 : 금오공과대학교 전자공학부 교수
<관심분야> 정보보안, 암호화 프로토콜

유제니오 (M. E. Morocho-Cayamcela)
2020년 8월 : 금오공과대학교 전자공학과 박사
2020년 9월~현재 : Yachay Tech University 컴퓨터 공학부 교수
<관심분야> 무선통신, 정보보안

김 명 식 (Myung-Sik Kim)
1992년 2월 : KAIST 전자공학과 박사
1992년 3월~현재 : 금오공과대학교 전자공학부 교수
<관심분야> 정보보안, 정보처리

임 완 수 (Wansu Lim)
2010년 8월 : GIST 정보통신공학과 박사
2014년 9월~현재 : 금오공과대학교 전자공학부 교수
<관심분야> 지능형 제어, 임베디드 시스템
[ORCID:0000-0003-2533-3496]