International Journal of Safety and Security Engineering
Vol. 11, No. 6, December, 2021, pp. 697-702
Journal homepage: http://iieta.org/journals/ijsse

RoundPIN: Shoulder Surfing Resistance for PIN Entry with Randomize Keypad

Seerwan Waleed Jirjees*, Ahmed Raoof Nasser, Ali Majeed Mahmood

Control and Systems Engineering Department, University of Technology, Baghdad 10066, Iraq

Corresponding Author Email: seerwan.w.jirjees@uotechnology.edu.iq

https://doi.org/10.18280/ijsse.110610

Received: 23 October 2021
Accepted: 12 December 2021

Keywords:
PIN entry, ATM security, shoulder surfing attack, authentication

ABSTRACT

The security of a PIN is largely supported by the authentication process in ATM. Most authentication methods like traditional are based on using PIN as direct entry and this technique has been shown lots of drawbacks such as vulnerability to password space, and shoulder-surfing. In this paper, a new approach is proposed called RoundPIN depends on the appearance of the numerical password through one of the buttons after selecting it by the user and it is done through a number of rounds, the numbers are arranged randomly on the keypad. Due to the variable aspect of the chosen button and the random appearance of the numbers in each connection session and also the selection process will take place through three buttons three auxiliary, the proposed approach can maintain high secure session to enter the PIN to resist shoulder surfing, which is difficult for attackers to observe a user's PIN. The performance evaluation of the proposed approach is achieved in two parts, the first one is based on security analysis. Then a pilot study of thirty users is conducted to evaluate the useability of the proposed approach. It is noticed that the proposed approach can maintain a high level of security as well as acceptable level of useability and user satisfaction compared the conventional keypad system.

1. INTRODUCTION

Authentication is a mechanism that confirms a user's identity and maintains network security by permitting only authenticated users to access protected resources [1, 2]. User authentication is an important component of most computer security systems since it offers one of the fundamental terms of user access control and accountability [3].

In fact, a Personal Identification Number (PIN) is normally produced and saved to be used as numerical passwords for user authentication and numerous unlocking functions. Because current touch screens make it easier to integrate a PIN entry interface on a range of commodity equipment and devices, such as Automated Teller Machines (ATMs) and point-of-sale terminals, their use is growing [4, 5]. The most common way to enter a PIN is to use the traditional keypad in ATM. Nevertheless, this increases the chance of attackers for hacking the password. A shoulder surfing attack can attain information for instance a PIN, passwords, and other private data thru direct observation while logging into the system [6, 7]. Especially in crowded environments, it may observe what the user has done on the screen while logging into the system [8, 9]. Indirect PIN entry methods are often used as a countermeasure to shoulder surfing attacks to achieve security even though they require a greater cognitive workload for users [10].

It is worth stating that the available entry methods that were used to protect the user's PIN from shoulder surfing attack are simple in design as well as they may have a low security process. This is due to that; the attacker can perform easily pin monitoring by surveillance cameras. On the other hand, some of the existing methods can provide a higher percentage of security, but the pin entry method is too complex and difficult to implement.

In this paper, a RoundPIN entry approach is proposed to achieve a higher level of password resistance against a shoulder surfing attack. RoundPIN combines both simplicity in implementation and a very high level of security as well. The key idea of the proposed RoundPIN system is to locate the user's PINs in a keypad with a changeable keys layout at each login session. This can increase the security of the pin entry with RoundPIN, since the pin entering process is indirect, unlike the traditional methods.

The results of evaluating the proposed RoundPIN approach by a number of participants illustrate the effectiveness of RoundPIN for resisting the shoulder surfing attacks through the experiment by either direct observation or by recording from surveillance cameras. Additionally, the results show the satisfaction of users in terms of PIN entry time and the ease of use compared to the traditional keypad. The remainder of this paper is structured as follows. Section 2 presents a literature review of the previous work. Section 3 describes the proposed RoundPIN approach. Performance evaluation and discussion are presented in Section 4. Finally, section 6 concludes the paper.

2. RELATED WORK

Several methods have been proposed to protect the users' PINs from shoulder surfing attacks, the login procedure is usually too long and the number of its rounds is multiple, which makes these schemes unsuitable, so the proposals should consider the requirements on security and easy to use. This section reviews and analyses the related studies of authentication techniques.

Kumar et al. [11] propose an authentication system based on eye password. This approach decreases the impact of shoulder surfing attacks. The user can choose the password characters from the screen's keypad using his eyes. The system then calculates whether it is correct or incorrect selection based on the user's eye orientation. The author claims the system reduced shoulder surfing, although the login session takes a long time. An authentication method is designed, where the process of selecting a PIN code or registering a PIN code consists of two parts [12, 13]. The user must first select a four-digit PIN code, identical to how they would with a standard PIN-based authentication mechanism. While the second stage requires the user to choose one of 40 available locations. The user can choose a location by clicking on it. However, the authentication procedure is quite long and the percentage of error is high in this method. De Luca et al. [14] suggest a system of three colors keypad called colorpin. Colors are characterized by alphabetic characters. At the stage of registration, the user has to choose the number and color, and then when entering, the letter that corresponds to the number and color will be pressed. The usage of numbers, colors, and characters in the system may make it difficult for the user to enter the PIN.

Similarly, the approach [15, 16] uses PIN pad buttons that are randomly divided into two groups based on their color. The user indicates the color group containing the digit for each PIN digit in numerous rounds. Although the user never explicitly enters the PIN, this method significantly increases the time required to enter the PIN. The authors find that their approach is more resistant to shoulder surfing than standard PIN entry in a small-scale trial (n=8). The proposed system consists of two interfaces, the first one is a visible user interface consisting from a grid of characters which allows the user to search for his/her password characters, which their location are obtained from the second hidden grid interface [17, 18]. The second one is a hidden interface that contains the same number of characters as the visible interface but the character's locations on the grid are different. The user will search for the characters in the visible interface and specify its location and then displays the hidden interface and write the password. Kasat and Bhadade [19] have tried to evaluate the performance of the TicToc PIN entry technique. It is based on the display of four colors below the numeric pad. The user then chooses a color and enters a numerical value at each step. To save mental effort and time, they proposed FlyWheel [19], a variation of Tictoc meant to increase security, usability, and minimum authentication time. Each numeric key in FlyWheel is identifiable by two colors; the user is prompted to choose between the two colors in order to input a value; the colors and layout are created randomly throughout each session. Although FlyWheel is less cognitive effort, its application on an alphanumeric keypad is complex. Additionally, it necessitates multiple actions to enter a single digit, as each one requires two user activities.

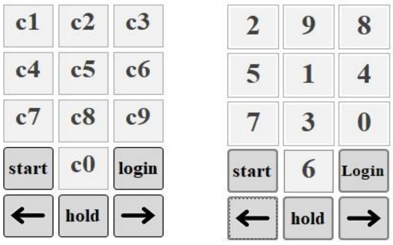
Unlike the above contributions, in this paper, the proposed approach provides a robust strategy to resist the shoulder surfing attack using the concept of random rounds keypad for password entry. In the RoundPIN approach, three types of PIN entry techniques are deployed. The proposal does not require the user to memorize anything other than the PIN. The designs close to the traditional keyboard make it easy to use and also the possibility of programming them simply on the systems, unlike the proposals whose designs are complex and difficult to implement and use.

3. THE PROPOSED ROUNDPIN APPROACH

The proposed system is a new approach that can solve the existing problem in the PIN entry particularly shoulder surfing attacks, The key idea depends on searching for the user's PIN through rounds on the keypad buttons which have to be arranged randomly at each new login session. The detail of the proposed RoundPIN approach will be described in the next subsections.

3.1 RoundPIN user interface

The design of the proposed keypad is based on the traditional numeric keypad with additional functional buttons. As shown in Figure 1, two of them are used to navigate between rounds. Additionally, the hold button is used to save the number of rounds. The start button is used to initialize the login session. The last one is the login button. It is worth stating that the details of the proposed keypad will be described completely in the next subsections.



(a) (b)

Figure 1. RoundPIN interface (a) the order of the button locations used to select the password button, (b) how the numbers are randomly displayed on the keypad

3.1.1 RoundPIN authentication phase

In the authentication phase, the registration, as well as the login sessions for the proposed RoundPIN authentication approach, are intended to be as possible simple and user-friendly. The login phase can be described as follows:

The login phase is divided into four steps as follows.

Step 1. User side: start to enter a PIN.

Step 2. ATM side: arranging the locations of the numbers on the keypad randomly shown in Table 1.

Table 1. Arranging the locations of the numbers on the keypad randomly

	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9
Round_1	8	4	1	0	7	3	6	9	5	2
Round_2	4	0	7	6	3	9	2	5	1	8
Round_3	6	2	9	8	5	1	4	7	3	0
Round_4	1	7	4	3	0	6	9	2	8	5
Round_5	7	3	0	9	6	2	5	8	4	1
Round_6	9	5	2	1	8	4	7	0	6	3
Round_7	5	1	8	7	4	0	3	6	2	9
Round_8	0	6	3	2	9	5	8	1	7	4
Round_9	3	9	6	5	2	8	1	4	0	7
Round_10	2	8	5	4	1	7	0	3	9	6

Step 3. User side: entering his\her PIN then login.

Step 4. ATM side: read the coding text, then use the first digit to indicate the column, the remaining digits provide the row value, which represents the round number, as shown in step 2. Then by intersecting the column and the row, the user

PIN will be obtained, if the PIN is matching with the stored database value, the connection is established, otherwise, authentication is rejected. Figure 2 summarizes the entire authentication process.

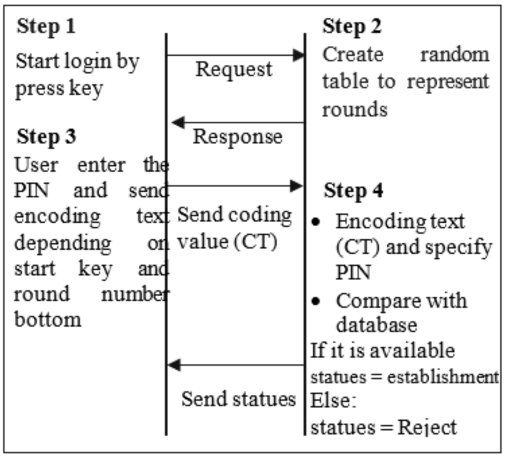


Figure 2. The structure of the authentication phase

3.1.2 RoundPIN entry method

The process of entering the password using the proposed approach can be summarized in the steps shown below. This process will prevent intruders who use shoulder surfing to know the numbers of the PIN and also give the user a safer session to enter his/her PIN.

Step 1. The user starts the login process by pressing the start button

Step 2. The user specifies the button in the keypad depending on one of the methods of selection button that shown earlier in Figure 1.

Step 3. the user looking for the first number of her/his PIN in the keypad by pressing the next key or back key (rounds), in case finding the number, the user will press the hold button, and the process will be repeated until all the numbers of PIN are found and hold.

Step 4. after the user enter all numbers of PIN in step 3, then will press the login button and waiting for the response from the ATM.

To illustrate the principle of the proposed RoundPIN pin entry approach for ATM, the following example is considered for the real password of a user which is (2013) and the start button is (C5) as shown in Figure 3.

- **User side(encoding)**: the user must specify the start button first then click the start key, after that the numbers will appear on keypad as shown in Figure 3, the user will be looking for the first PIN value that will find it in round 5 and he press hold key to save it then press next key to find second PIN value and he is found it in round 7 and continuous search by press next or back key to complete all PIN values. After pressing login key the value that will be sent is "55731" which means the first digit is the location of the key that specified by the user and the other digits represent the number of rounds respectively
- **ATM side(decoding)**: Depending on the first digit, it will select column 5 that shown in Table 1 and the others digits represent the numbers of row. The intersection of the row and column will represent the user's password.

3.2 RoundPIN selection start button

Before starting the process of entering the PIN through the rounds, a button has to be selected by the user as a reference location on the keypad for PIN entry. Three scenarios are suggested for the method of selecting the aforementioned button as shown in Figure 4. The suggested scenarios are described as follows:

- RoundPIN-Click: Figure 4a shows the method of selecting the button by pressing it through the keypad directly. This method is considered easy and clear by the user, nevertheless, the security aspect is low due to the possibility of the attacker noticing the chosen button.
- RoundPIN-Hidden: In this technique, the system will suggest the location of the button randomly when the user presses the start button. The selected button number will appear next to the start button in a faded small font for a short period of time and as shown in Figure 4b. This method is safer than the former one (RoundPIN-Click), due to the difficulty of noticing the button number that appears on the screen by the attacker.
- RoundPIN-SMS: Here the customer service center will be requested by the user to provide a text message that shows the number of the selected button for entering the PIN as shown in Figure 4c. Although this method may take a longer time in the login process; it can provide higher security compared to the two previous methods.

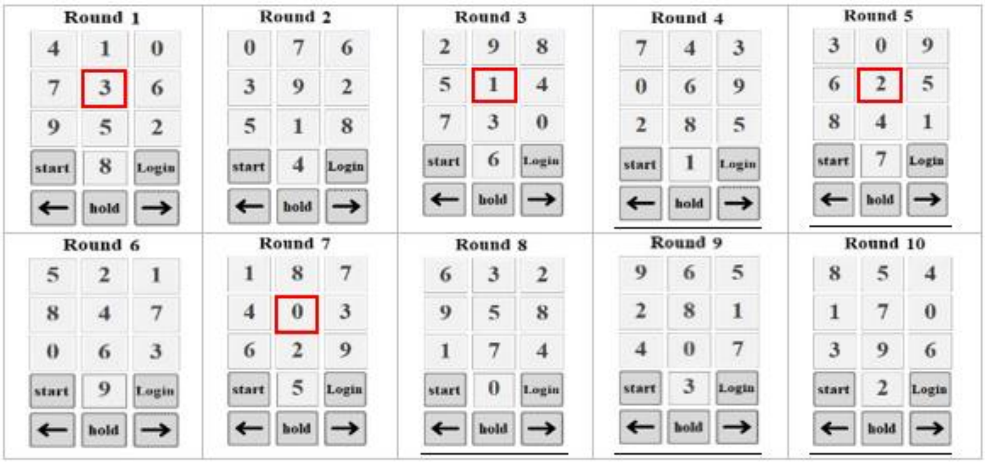
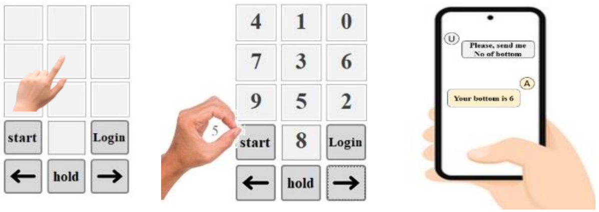


Figure 3. An example of the proposed approach's rounds



(a) (b) (c)

Figure 4. Types of methods used to select the start button. (a) RoundPIN-Click; (b) RoundPIN-hidden; (c) RoundPIN-SMS

4. PERFORMANCE EVALUATION AND DISCUSSION

This section will focus on evaluating the effectiveness of the proposed approach based on different aspects which include security analysis and useability analysis. The evaluation is achieved via conducting a pilot study involving a number of participants. The pilot study is conducted by engaging 20 participants (12 male, 8 female, average age: 22 to 40) for testing the proposed RoundPIN method in real life scenarios.

4.1 Usability analysis

For testing the system useability, the participants in the pilot study have received an overview of the study. This involves the parts and the entry form that is explained in detail for each of them. The pilot study includes a questionnaire that collects basic demographic data as well as information about experiencing the use of RoundPIN from the participant's point of view.

The proposed method is implemented in C sharp environment for windows OS using a touchscreen computer. two independent variables are set, PIN type (system-chosen PIN, user-chosen PIN) and PIN entry system (RoundPIN_Click, RoundPIN_Hidden, RoundPIN_SMS). Different metrics such as password entering delay, number of mistakes in password entering, and the system complexity from user's perspective, are used to analyze the usability of the systems [20, 21].

4.1.1 Entry time

The authentication timings for the authentication mechanisms in combination with PIN type (user-created PINs, random PINs) and PIN entry system (traditional PIN, RoundPIN) are depicted in Figure 5. The traditional PIN (supplied by the user) was the quickest (mean: 1.41s, sd: 0.79s), followed by the random traditional PIN (mean: 1.79s, sd: 0.45s). RoundPIN with a randomly created PIN was the slowest technique (mean: 15.5s, sd: 5.23s) and was somewhat slower than RoundPIN with a randomly generated PIN (mean: 17.92s, sd: 1.84s).

4.1.2 Error rate

The results in Figure 6 show the error rate of the input method of the proposed system compared to the normal input method. In the traditional PIN entry, each participant can successfully authenticate with the system on the first attempt. We measured whether the participant can authenticate correctly with the proposed system within the first attempt and how many failed attempts. It is noticed that there are six failed attempts by 4 users nonetheless with an increasing number of attempts up to the five attempts, there is only one failed attempt. The number of mistakes in password entering is calculated for each participant as shown in Figure 6.

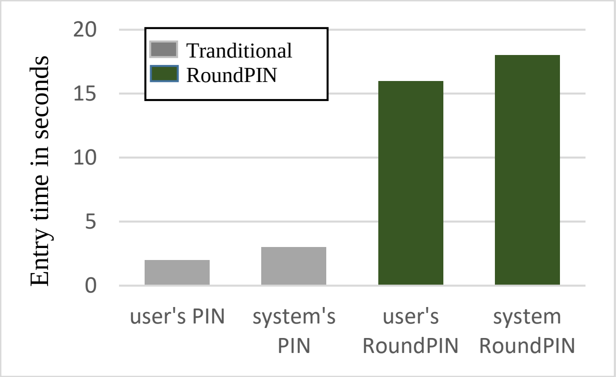


Figure 5. Successful authentication entry time

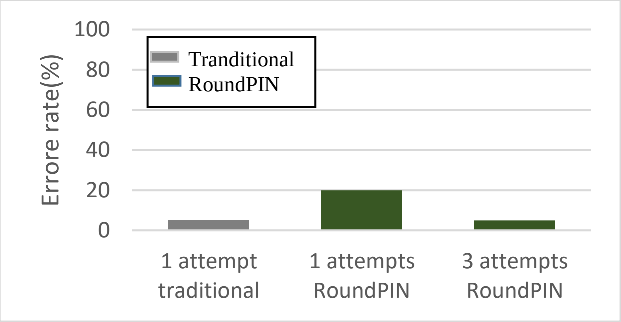


Figure 6. PIN entering errors

4.2 Security analysis

In a shoulder surfing attack, the attacker tries to obtain the password by following the user while logging into the system. Especially in crowded environments, by bringing it closer to the aggressive user and the screen, it can observe what the user has done while logging into the system [22, 23].

In the proposed approach, the process of stealing the PIN is very difficult with a one-time attack or several times because the arrangement of numbers on the keypad and for all rounds appears randomly at the beginning of each entry. In addition, it is possible to hide the movement of the hand when pressing the three basic keys used to enter the password

To evaluate the performance of the proposed approach, a test was conducted to analyze the security aspect of the system and its resistance to shoulder surfing attacks by 20 participants on the three proposed scenarios that are mentioned earlier in section 3.2. The results showed that out of 60 real authentication sessions with entering the traditional PIN were 56 successful sessions for the type of RoundPIN-Click and 59 successful sessions with the RoundPIN-Hidden, and all the sessions were successful for the RoundPIN-SMS type.

Moreover, when video attacks are used via surveillance camera, where the video clips are shown to the participants with the possibility of pausing and rewinding. For each entry, with slow entry and no masking of hand movement, attackers were able to guess 7 entries for RoundPIN-Click. Also, 4 entries were guessed for RoundPIN-Hidden type, but they could not guess any RoundPIN-SMS attempt.

Furthermore, the same people in the previous test that the attackers have guessed their PIN's were trained in a way that could hide the movement of the hand on the buttons (by placing the palm of the other hand on the fingers of the hand that is used to enter the password) in the RoundPIN-Click and RoundPIN-Hidden and then trying to use video-style attacks again, were observed that the attackers are unable to notice or guess the password. Figure 7 security analysis of RoundPIN types.

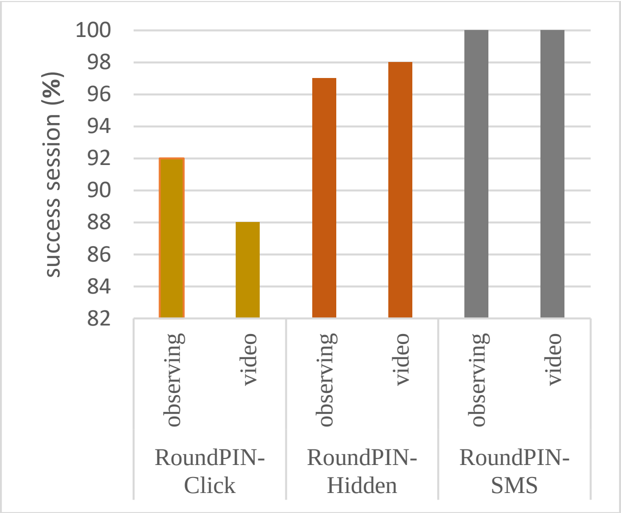


Figure 7. Security analysis of three RoundPIN types

5. CONCLUSION

Shoulder surfing is one of the key challenges that may face security systems. Attackers can steal the user's PIN when it displays in the user's vicinity. In this paper, the RoundPIN input scheme is proposed in which the design of the input interface is similar to the traditional input interface. The scheme companies both the simplicity of use with high security against guesswork and over-the-shoulder attacks. This can maintain by changing the locations of the input numbers on each new connection request. In RoundPIN, the entry process is also indirectly on the buttons, where three techniques are suggested to determine the start button to increase the resistance against the shoulder surfing attack, which are RoundPIN-Click, RoundPIN-Hidden, and RoundPIN-SMS. Although the results are acceptable with the RoundPIN-Click and the RoundPIN-Hidden, nonetheless the third RoundPIN-SMS is the best one since no case of hacking has occurred in tests. The results of the evaluation test for several participants demonstrate that the RoundPIN approach maintains high resistance against shoulder surfing attacks. Furthermore, the RoundPIN has high satisfaction of users due to its ease of use compared to the usual keyboard. The proposed system can be used in further applications such as mobile phones, credit cards and banking. The RoundPIN can be extended to involve both numbers and letters. One of the challenges that have been faced during the application of the RoundPIN approach is the delay for the first time use in entering the PIN and this can be managed and resolved with frequent use and practice for the new users.

REFERENCES

[1] Shivaprasad, G. (2019). Research and development of user authentication using graphical passwords: A prospective methodology. International Journal of Innovative Technology and Exploring Engineering, 8(9s3): 385-390. https://doi.org/10.35940/ijitee.I3071.0789S319

[2] Subangan, S., Senthooran, V. (2019). Secure authentication mechanism for resistance to password attacks. In 2019 19th International Conference on Advances in ICT for Emerging Regions (ICTer), 250: 1-7. https://doi.org/10.1109/ICTer48817.2019.9023773

[3] Wang, C., Wang, Y., Chen, Y., Liu, H., Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. Computer Networks, 170: 107118. https://doi.org/10.1016/j.comnet.2020.107118

[4] Chabbi, S., Boudour, R., Semchedine, F., Chefrour, D. (2020). Dynamic array PIN: A novel approach to secure NFC electronic payment between ATM and smartphone. Information Security Journal: A Global Perspective, 29(6): 327-340. https://doi.org/10.1080/19393555.2020.1773583

[5] Rajarajan, S., Priyadarsini, P. (2019). UTP: A novel PIN number based user authentication scheme. The International Arab Journal of Information Technology, 16(5): 904-913.

[6] Lai, J., Arko, E. (2021). A shoulder-surfing resistant scheme embedded in traditional passwords. In Proceedings of the 54th Hawaii International Conference on System Sciences, pp. 7144-7152. https://doi.org/10.24251/HICSS.2021.860

[7] Fong, T.J., Abdullah, A., Jhanjhi, N.Z., Supramaniam, M. (2019). The coin passcode: A shoulder-surfing proof graphical password authentication model for mobile devices. International Journal of Advanced Computer Science and Applications (IJACSA), 10(1): 302-308. https://doi.org/10.14569/IJACSA.2019.0100140

[8] Panda, S., Kumari, M., Mondal, S. (2018). SGP: A safe graphical password system resisting shoulder-surfing attack on smartphones. In International Conference on Information Systems Security, pp. 129-145. https://doi.org/10.1007/978-3-030-05171-6_7

[9] Prabhu, K.D.D.P. (2018). Image based authentication using illusion pin for shoulder surfing attack. International Journal of Pure and Applied Mathematics, 119(7): 835-840.

[10] Revathy, R., Bama, R. (2015). Advanced safe PIN-Entry against human shoulder-surfing. IOSR Journal of computer Engineering, 17(4): 9-15.

[11] Kumar, M., Garfinkel, T., Boneh, D., Winograd, T. (2007). Reducing shoulder-surfing by using gaze-based password entry. In Proceedings of the 3rd Symposium on Usable Privacy and Security, pp. 13-19. https://doi.org/10.1145/1280680.1280683

[12] Salman, M., Li, Y., Wang, J. (2019). A graphical PIN entry system with shoulder surfing resistance. In 2019 IEEE 4th International Conference on Signal and Image Processing (ICSIP), pp. 203-207. https://doi.org/10.1109/SIPROCESS.2019.8868388

[13] Shi, P., Zhu, B., Youssef, A. (2009). A rotary pin entry scheme resilient to shoulder-surfing. In 2009 International Conference for Internet Technology and Secured Transactions(ICITST), pp. 1-7. https://doi.org/10.1109/ICITST.2009.5402625

[14] De Luca, A., Hertzschuch, K., Hussmann, H. (2010). ColorPIN: Securing PIN entry through indirect input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1103-1106. https://doi.org/10.1145/1753326.1753490

[15] Roth, V., Richter, K., Freidinger, R. (2004). A PIN-entry method resilient against shoulder surfing. In Proceedings

of the 11th ACM Conference on Computer and Communications Security, pp. 236-245. https://doi.org/10.1145/1030083.1030116

[16] Kim, C.S., Lee, M.K. (2010). Secure and user friendly PIN entry method. In 2010 Digest of Technical Papers International Conference on Consumer Electronics (ICCE), pp. 203-204. https://doi.org/10.1109/ICCE.2010.5418819

[17] Kwon, T., Na, S. (2015). SteganoPIN: Two-faced human–machine interface for practical enforcement of PIN entry security. IEEE Transactions on Human-Machine Systems, 46(1): 143-150. https://doi.org/10.1109/THMS.2015.2454498

[18] Kwon, T., Na, S. (2014). SwitchPIN: Securing smartphone PIN entry with switchable keypads. In 2014 IEEE International Conference on Consumer Electronics (ICCE), pp. 23-24. https://doi.org/10.1109/ICCE.2014.6775892

[19] Kasat, O.K., Bhadade, U.S. (2018). Revolving flywheel pin entry method to prevent shoulder surfing attacks. In 2018 3rd International Conference for Convergence in Technology (I2CT), pp. 1-5. https://doi.org/10.1109/I2CT.2018.8529758.

[20] Still, J.D., Bell, J. (2018). Incognito: Shoulder-surfing resistant selection method. Journal of Information Security and Applications, 40: 1-8. https://doi.org/10.1016/j.jisa.2018.02.006

[21] Srinivasan, R. (2018). DragPIN: A secured PIN entry scheme to avert attacks. Int. Arab J. Inf. Technol., 15(2): 213-223.

[22] Alsuhibany, S.A. (2020). Usability and shoulder surfing vulnerability of pattern passwords on mobile devices using camouflage patterns. Journal of Ambient Intelligence and Humanized Computing, 11(4): 1645-1655. https://doi.org/10.1007/s12652-019-01269-3

[23] Khedr, W.I. (2018). Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol. Journal of Information Security and Applications, 39: 41-57. https://doi.org/10.1016/j.jisa.2018.02.003