ISSN 2320 - 2602
Volume 9 No.7, July 2020
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst06972020.pdf
https://doi.org/10.30534/ijacst/2020/06972020

Gaze Based Password Entry using Android: Pin Based Authentication Methods to Reduce Shoulder Surfing Attacks

Devipriya S Kumar[1], Fincy Joseph[2], Mary Nimisha[3], Sreelakshmi S Nair[4], Ms.Gayathri R Krishna[5]
[1]Mangalam College of Engineering, India,devipriyasreeragam@gmail.com
[2] Mangalam College of Engineering, India, fincyjoseph1996@gmail.com
[3]Mangalam College of Engineering, India, marynimisha1996@gmail.com
[4]Mangalam College of Engineering, India, sreelakshmi.malikayil@gmail.com
[5] Mangalam College of Engineering, India, gayathri.krishna@mangalam.in

ABSTRACT

The paper addresses the problem of shoulder-surfing attacks on authentication schemes by proposing Illusion PIN (IPIN), a PIN-based authentication method that operates on touch screen devices. IPIN blends two keypads with different digit ordering with the help of hybrid images in such a way that the user who is close to the device is seeing one's keypad to enter their PIN, while the attacker who is looking at the device from a long distance is seeing only the other's keypad. It uses shuffling algorithms to shuffle the keypad since the attacker may memorize the spatial arrangement of the pressed digits. To improve the security of Illusion PIN, an algorithm is used which is based on human visual perception. By the end, the project quantified the level of resistance against shoulder- surfing by introducing the notion of safety distance, which is estimated with a visibility algorithm.

Key words: Authentication PIN, Hybrid Images, Human Visual Perception, Shoulder-surfing, Video Attack.

1.INTRODUCTION

1.1 Overview of Illusion

For instance, a baby who perceives tree branches in dark as if they are goblins could also be said to behave an **illusion**. The design of **Illusion PIN** is predicated on the straightforward observation that the user is often viewing the screen of the user device from a shorter distance than a shoulder-surfer. The **core idea of Illusion PIN** is to create the keypad on the touch screen to be interpreted with a unique digit ordering [10]. The user's keypad is shuffled in every authentication attempt.

1.2 Overview of Shoulder Surfing

In computer security, **shoulder surfing** is a type of social engineering technique used to get information like personal identification number (PINs), passwords and other confidential data by looking over the victim's shoulder, either from keystrokes on a tool or sensitive information being spoken and heard, also known as eavesdropping Figure 1.

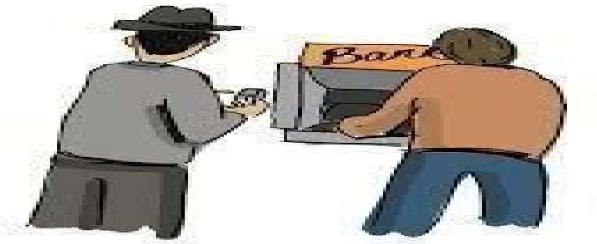


Figure 1: Shoulder Surfing Attack

The main measures of shoulder surfing are

- Gaze-based password entry
- Secret tap method
- Comparison of risks between alphanumeric & graphical
- PIN entry

1.2 GAZE based Password Entry

The basic procedure is that reminiscent to normal password entry, except that in situation of typing a key or touching the screen, the user looks at each desired character or trigger region in sequence (same as eye typing) [9]. The approach can, therefore, be used both with character-based passwords by using an on-screen keyboard and with a graphical password scheme.

1.3 Secret Tap Method

In computer security, shoulder surfing is a type of social engineering technique used to get information like personal identification numbers (PINs), passwords and other confidential data by looking over the shoulder of the victim, either from keystrokes on a device or sensitive information being spoken and heard, also known as eaves dropping. This attack is performed either at close range(by directly looking over the victim's shoulder) or from a longer range. To apply this technique attackers do not require any technical skills; keen observation of victims' surroundings and the typing pattern is required [7]. Therefore, it is important to make the authentication process more complex in order to prevent authentication information from being stolen even if cameras and/or other individuals sees the information input process numerous times. One of the simplest forms of a secret tap method is biometrics such as fingerprint scanning or facial recognition, which cannot be replicated by an attacker [4].

1.4 Comparison of Risks

The key advantage of the graphical password compared to the alphanumeric password is that the improved memorability. However, the potential detriment of this advantage is that the increased risk of shoulder-surfing. The result indicates the very fact that both alphanumeric and graphical password-based authentication mechanisms may have significant vulnerability to shoulder-surfing unless certain precautions are taken [6]. Despite the common belief that non-dictionary passwords are the foremost secure kind of password-based authentication; results demonstrate that it's, in fact, the foremost vulnerable configuration toshoulder-surfing.

1.5 PIN Entry

A **personal identification number** (**PIN**), or sometimes redundantly **PIN**, may be a numeric or alpha-numeric password employed in the method of authenticating a user accessing a system. The personal identification number has been the key to flourishing the exchange of PIN data between different data-processing centers in computer networks for financial institutions, governments, and enterprise [5].

2.BLOCK DIAGRAM

The Figure 2 indicates the working of illusion pin and its flow of functions.

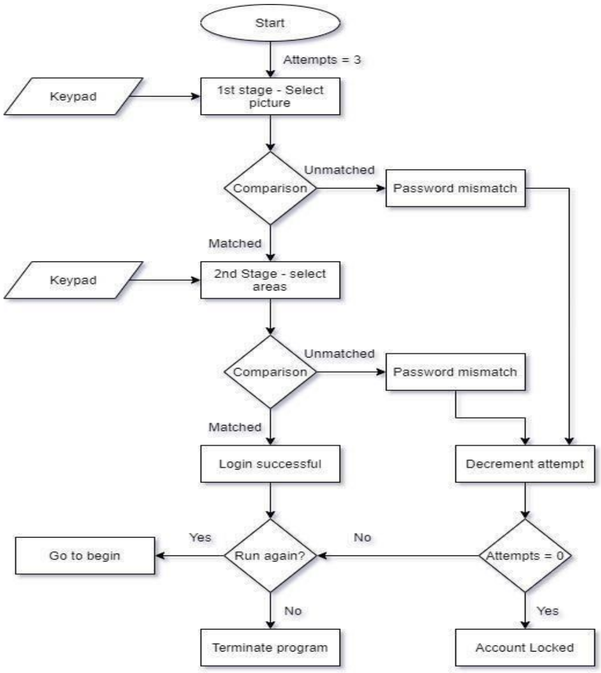
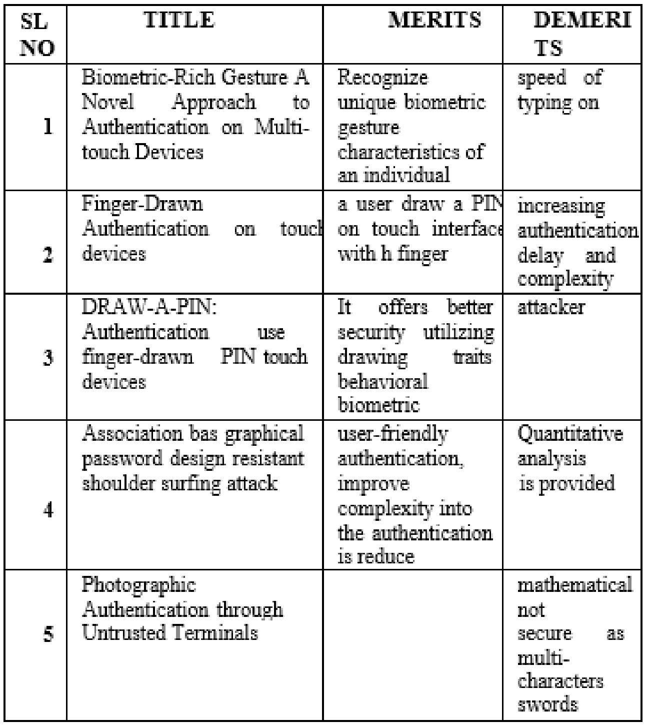


Figure 2: Working of illusion pin

3. LITERATURE SURVEY

Table 1: Literature Survey



SL NO	TITLE	MERITS	DEMERI TS
1	Biometric-Rich Gesture A Novel Approach to Authentication on Multi-touch Devices	Recognize unique biometric gesture characteristics of an individual	speed of typing on
2	Finger-Drawn Authentication on touch devices	a user draw a PIN on touch interface with h finger	increasing authentication delay and complexity
3	DRAW-A-PIN: Authentication use finger-drawn PIN touch devices	It offers better security utilizing drawing traits behavioral biometric	attacker
4	Association bas graphical password design resistant shoulder surfing attack	user-friendly authentication, improve complexity into the authentication is reduce	Quantitative analysis is provided
5	Photographic Authentication through Untrusted Terminals		mathematical not secure as multi-characters swords

In Table1. It shows the comparison of the 5 similar related method which taken for the project and its basic characteristics are listed.

4. PROBLEM STATEMENT

Existing systems only provide some authentication techniques using pattern recognition schemes and it does not provide complete resistance to shoulder surfing. It only makes a way to recognize patterns or personal photographs of users and ask them to identify their own personal photographs from a set of images.This may cause an attacker to memorize the patterns or photographs and the solutions need to provide more resistance to shoulder surfing. There should be a solution to shuffle the keypads so that the attacker may not memorize it [2].

The motivation behind the project is the need for resistance to various shoulder surfing attacks faced nowadays. Since having different old technologies for shoulder surfing attacks, illusion pin comes with an authentication scheme to blend two keypads of different digit ordering to a single hybrid image to provide more security with the feature of shuffling keypads. The main aim of this project to avoid hacker's attack. here it's a practically impossible at the user can observer the device within in the bigger distance [3].so the user cannot understand what are often done on the system. If an attacker can see the pin authentication of the user that the attacker imitates the pin authentication by an assumption. To satisfy the wants of users to extend shoulder surfing resistance without the usability overhead. Address the matter of shoulder surfing attacks on authentication schemes by proposing IPIN. Such some way that the user who is near the device is seeing on the keypad to enter the PIN, while the attacker who is starting at the device from an even bigger distance is seeing only the oppositekeypad.

5. PROPOSED SYSTEM

Traditional password authentication into a computer system with a keyboard is vulnerable to shoulder surfing attacks. Shoulder surfing refers to the usage of observation techniques i.e. looking over someone shoulder, to obtain their password [1]. In the proposed method, created a virtual keypad with a deceptive visual impression PIN. The virtual keypad is composed of two keypads with alternative digit orderings, combined in a single hybrid image. The keypad shows different values for user and attacker based on visibility algorithm that considers distance as a major factor for keypad changing Figure3.

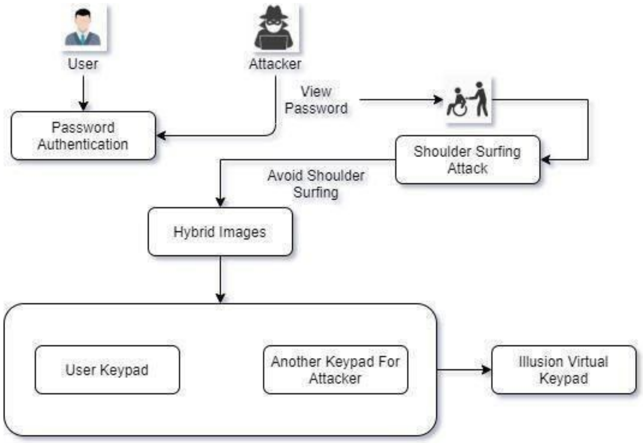
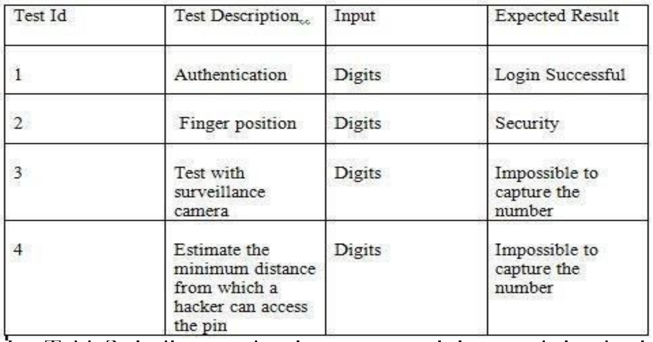


Figure 3: . Block diagram of user password authentication

Gaze tracking works by using computer vision techniques to track the orientation of the user's pupil to calculate the position of the user's **gaze** on the screen. **Gaze-based password entry** makes gleaning **password** information difficult for the unaided observer while retaining the simplicity and ease of use for the user.

6. TEST CASES

Table 2: Test Cases



Test Id	Test Description	Input	Expected Result
1	Authentication	Digits	Login Successful
2	Finger position	Digits	Security
3	Test with surveillance camera	Digits	Impossible to capture the number
4	Estimate the minimum distance from which a hacker can access the pin	Digits	Impossible to capture the number

In Table2 indicates the inputs we giving and its basic performance tasks. Here system performs authentication, finger position recognition, test with surveillance camera and estimate minimum distance from which a hacker can access the pin. Several inputs are given and finally how the output is successfully run by the system is shown.

7. EXPERIMENT RESULTS

In Figure4, it indicates the whole analysis of the system based on security is shown.

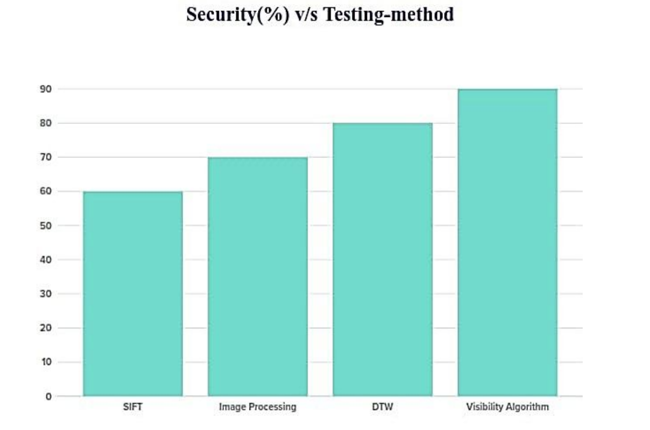


Figure 4: Experiment results

8. CONCLUSION AND FUTURE SCOPE

In future, Illusion PIN creates for android application. This can help to enhance mobile security. Illusion poses have variety of interesting questions, which warrant further investigation. Recall that scheme doesn't mandate a given image processing filter the selection of an oil painting filter has been driven mostly by heuristic considerations. Further experimentation is additionally needed to raised evidence the re-silence of the scheme to some kinds of attacks the low fidelity test conducted to see optimal parameter selection, while highly encouraging, has to be expanded to supply stronger statistical evidence that attackers don't seem to be easily able to revert a distorted image back to its original meaning.

While investigating how best to tune filter during the course of prototype design and implementation discovered that finding an optimal parameter point for the lossy filter depends on the image to be transformed. It can be concluded that the visibility index threshold value isn't universal. It also wishes to remind that the values of the DAF filter parameters depend up on the task at hand. As a result, it should to repeat the estimation process for a considerably different task [8]. Then it is often concluded that the visibility algorithm may be accustomed assess the visibility of general images, but its parameters should be appropriately tuned for the actual task athand.The main goal of work was to provide a line-based authentication scheme which can be used to resist shoulder surfing attacks.The proposed system uses Illusion pin, apin-based authentication method that uses the technique of blending hybrid images with two different digit orderings into a single image. It is used mainly in touch screen devices. It allows a person to resist from shoulder surfing attacks by providing two blended keypads for one who is standing nearby it and other who is standing in a particular distance which is usually the attacker.

The system provides complete security to shoulder surfing attacks by shuffling the keypads using an algorithm so that the attacker cannot easily memorize the pin. conclude that the above method can be widely used to resist shoulder surfing attacks. The shuffling algorithm can widely be used to shuffle images but its parameters have to be tuned for the particular task inhand.

ACKNOWLEDGEMENT

We thank Department of Computer Science faculties and non- teaching staffs of Mangalam College of Engineering for permitting us to carry out this paper. Sincerely express our gratitude to all respected personalities who had guided and helped us in the completion of this paper.

REFERENCES

1 J Bonneau, C Herley, PC Van Oorschot, F Staino, the quest to replace passwords: A frameworks for comparative evaluation of web authentication schemes, in Security and Privacy (SP), 2012 IEEE Symposium on IEEE, 2012, pp. 553-567

2 M Harbach, A De Luca, S Eglman,theanatomyofsmartphoneunlocking,inProceedingsofthe 34th Annual ACM Conference on Human Factors in Computing Systems, CHI,2016.

3 R Anderson, why cryptosystems fail, in Proceedings of the 1st ACM Conference on Computer and Communication Security, ACM 1993, pp.215-227

4 A J Aviv, K Gibson, E Mossop, M Blaze and J M Smith, Smudge attacks on smartphone touch screens, WOOT, vo110, pp.1-7, 2006

5 A Olivia, A Torrabla, P G Schyns, Hybrid images, ACM Transaction on graphics (TOG), vol 25, no.3, pp 527-532, 2006

6 D Kim, P Dunphy, P Briggs, J Hook, J W Nicholson, P Olivier, Multi-touch authentication on

7 N H Zakaria, D Griffins, S Brostoff, J Yen, Shoulder surfing defense for recall based graphical passwords, in Proceedingsof the seventh Symposium on usable privacy and security, ACM, 2011, p6

8 I Jenrnyn, A J Mayer, F Monrose, M K Reiter, A D Rubin, The design and analysis of graphical passwords, In use Nix Securtiy, 1999

9 E Hayashi, R Dhamija, N Christin, A perring, **use of illusion: secure authentication usable everywhere**, Proceedings of the 4th symposium on the usable privacy and security, ACM, 2008, pp35-45

10 J Bonneau, S Preibusch, **the security of the customer- chosen banking plus**, I Financial Cryptography and data security, Springer Berlin Heidelberg 2012, vol7397, pp25-40