DECEPTIVE VISUAL IMPRESSION TO PREVENT SHOULDER SURFER ATTACK

Kalaichelvi[1], Raghav kumar[2], Ravikumar[3], Sathish kumar[4]

[1]Assistant Professor, Department Of ECE, V.S.B Engineering College, Karur, Tamil Nadu, India
[2,3,4]UG Students, Department of ECE, V.S.B Engineering College, Karur, Tamil Nadu, India

---

Abstract- *Nowadays shoulder surfer attack is a big threat for password authentication process. Authentication based on passwords is used largely in applications such as mobile phones, computer security and banking systems. For an attacker, it is too easy to crack the password in more densely populated area. To overcome this problem we proposed a deceptive visual impression PIN for password authentication process. We are using the concept of hybrid image in virtual keypad to make password authentication more secure.*

***Key Words*- Shoulder-Surfing, Hybrid Image, Human Visual Perception, PIN Authentication, Video Attack, Deceptive visual impression**

1. Introduction

Shoulder surfer attack is the act of stealing and spying others personal identification such as passwords and other details by standing back from the person. Authentication methods which are not strong to monitoring are sensitive to shoulder surf. Attackers can also do shoulder surfing in long distance by using binoculars and other viewing devices. It is an effective way to get the information and easily crack their required information such as banking details. When someone is unlocking their mobile phone on the street or in the subway, shoulders surfing is facilitated in such scenarios since it is easier for an attacker to stand close to the user while escaping people's attention. Shoulder surfer attackers are mainly focused on ATM machines to know debit card pin and their details. They are also using hidden cameras in their shirts to capture. We are proposed the virtual keypad for touch screen devices. It is in combination of two keypads and it is used in the form of soft keypad, which appears on a display screen for pin authentication. So we implemented the hybrid image concept to control the shoulder surfer attack problem. Hybrid image is nothing but it is an image consists of two different images in a single image based on the viewing angle and distance we can view any one image at a time**.**

2. OBJECTIVE

The main objective is to prevent shoulder surfing attack and make password authentication more secure. We are using the concept of deceptive visual impression concept in hybrid image. The method consists of hybrid image to blend two keypads with different digit orderings for each authentication process. The person who is going to enter the pin is able to view one keypad and the person who is standing behind the user able to view the other keypad at a time. It is based on distances of two persons with respect to the virtual keypad. We used an algorithm to determine whether the user keypad is visible to the person at a certain distance.

3. LITERATURE SURVEY

From the literature survey we have selected the base paper entitled as "An Improved Graphical Authentication System to Resist the Shoulder Surfing Attack"(IEEE 2017 International Conference on Technical Advancements in Computers and Communications). It is a method that uses graphical password authentication to resist shoulder surfing.

The paper titled as "Preventing Shoulder Surfing using Randomized Augmented Reality Keyboard (IEEE 2017 AnindyaMaiti, MurtuzaJadliwala and Chase Weber Electrical Engineering and Computer Science Department Wichita State University, USA). It consists a augmented reality wearable devices that shows the keypad arrangement in random manner.

The paper titled as "Invisible Secure Keypad Solution Resilient against Shoulder Surfing Attacks"(Div. of Undeclared Majors, Chosun Univ., Gwangju, South Korea, 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing). It describes the comparison of several authentication schemes and develops anti shoulder surfing security solution.

4. EXISTING METHOD

A Personal Identification Number (PIN) is a sequence of digits that checks the identity of a user when it is successfully entered. The development of pin authentication is a result of its continuous usage for many years in a wide range of day-to-day life applications like mobile devices, computers and banking systems.

In the existing method, shoulder surfing can be resisted by many ways. There is a method known as random keypad arrangement for password authentication process. The Obscurity method defines that the visual data of information has to be obscured. For example, Shield pin requires the person to physically cover the keypad by cupping one hand while using the other hand to enter the PIN.

The Visual Complexity method defines that it has to be difficult to receive the visual data interest. For example, graphical password authentication that allows the person to create a free form drawing on a touch screen devices and use it as user password.

In the above existing methods, the main drawback is we can easily capture the details by using video recording cameras. Those above methods cannot resist the shoulder surfer attack in a complete manner. Due to this reason, we implemented the virtual keypad based on hybrid images.

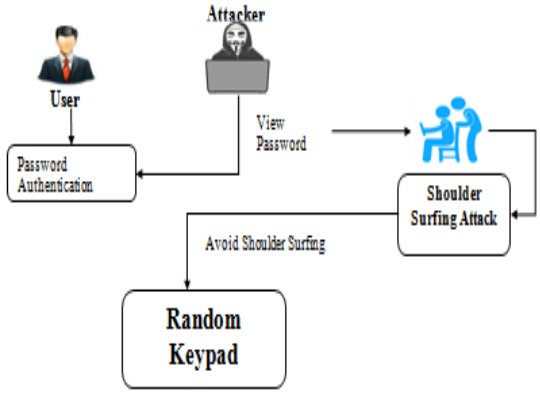


Fig a) Existing method diagram

5. PROPOSED METHOD

In proposed, we created the virtual keypad with 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 consider distance as major factor for keypad changing.

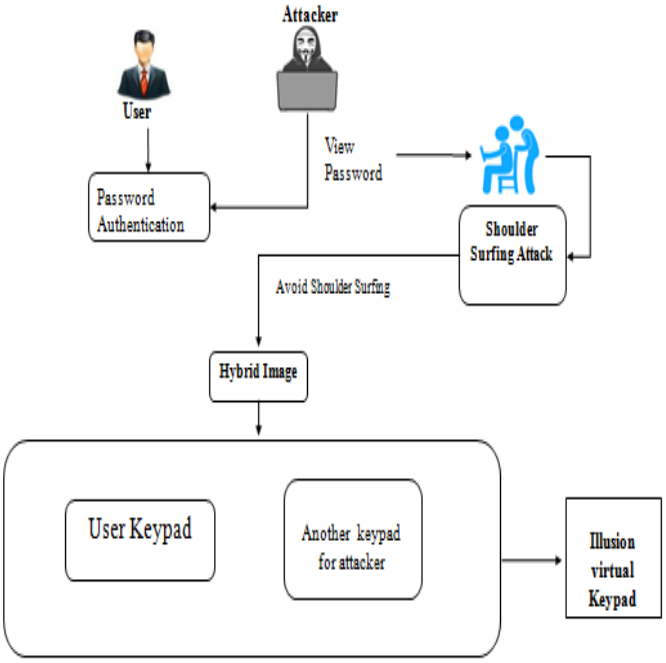


Fig b) Proposed method diagram

The visibility algorithm is mainly used to create the deceptive visual impression keypad. It determines whether the keypad is visible to a certain distance or not. It consists of the following steps:

1. Distance as filtering
2. Visibility Index
3. Threshold value of the visibility index

6. ALGORITHM EXPLANATION

The visibility algorithm receives input as a hybrid image and a viewing distance for the keypad. It returns the binary prediction values to ensure the user keypad is visible to a respective distance or not.

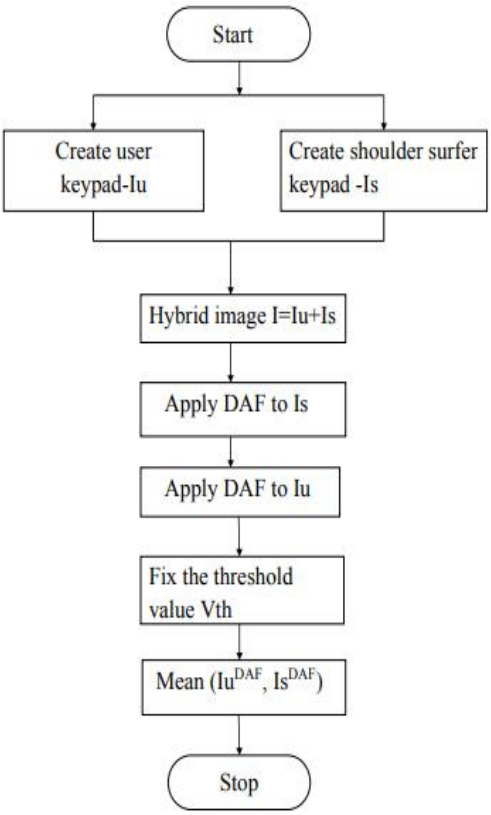


Fig c) Flow Chart

6.1. Distance as filtering:

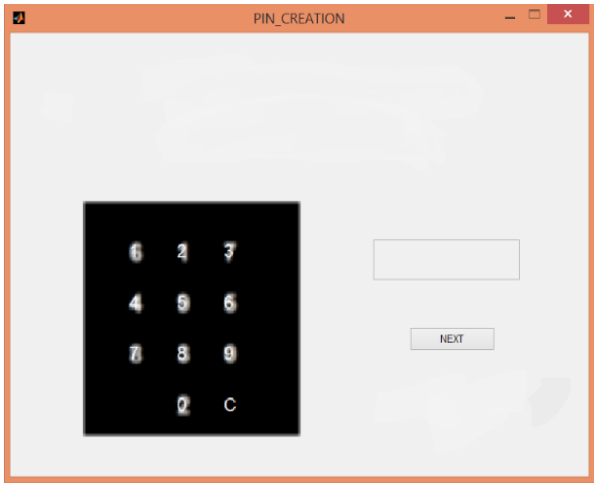
In this step, we need to stimulate the user keypad from the viewing position at a certain distance. It is done by filtering the image. The distance as filtering defines that we can stimulate the way in which the image is viewed at a particular distance filtering the image by using low pass filter. Every observer was looking directly at an image and his viewing position was completely defined by his viewing distance. Perception of an image depends on the visual angle, no matter where the observer stands.

6.2. Visibility Index:

The visibility index is the corner stone of our algorithm and we would like to clarify its behavior and the intuition behind it. The visibility index is the mean value of the 10 MSSIM (mean structural similarity index) values the pairs of corresponding buttons. The maximum value of the threshold value is 1. It is obtained when the user keypad is out of distance. One of the additional advantages is that the MSSIM is easily calculated.

6.3. Threshold value of a visibility index:

Based on the visibility index we set threshold Vth value when a particular observer is able to marginally recognize the digits of a user's keypad. Then, the visibility algorithm calculates the visibility index for the inputs I and N. Then we compare it with vth. If v>=vth, we determine user keypad cannot be viewed by the observer. If $v<=v_{th}$, we determine that the person is able to determine the digits of a users keypad. Since the threshold value will vary for different observers and corresponds to people with strongest vision



7. CONCLUSION

To this end we created the deceptive visual impression pin and the virtual keypad for the personal identification number validation have high resistant on shoulder surfer attacks. We increased the level of security to prevent shoulder surfer attacks. We implemented visibility algorithm in hybrid image to combine the keypads and to show the user keypad at a certain distance. It can also provide high security to user login pattern. The visibility algorithm gives a better visual representation during keypad authentication and the keypad gets shuffled after every authentication.

8. FUTURE WORK

In future work, we can create this deceptive visual impression technique in alphabets and we will implement this technique in android application to improve mobile security.

9. REFERENCE

[1] N. K. Ratha, J. H. Connell, R. M. Bolle , "Enhancing security and privacy in biometrics-based authentication systems": 2012 IEEE Symposium on. IEEE, 2012, pp. 553–567.

[2] M. Harbach, A. De Luca, and S. Egelman, "The anatomy of smartphone unlocking," in Proceedings of the 34th Annual ACM Conference on Human Factors in Computing Systems, CHI, 2016.

[3] Asher D'Mello, RohanBagwe, Victor Fernandes, AnkitaKaria, "Graphical Password Authentication Implementation and Evaluation of Personalized Persuasive Cued Click Points" : 2012, vol. 7397, pp. 25–40.

[4] R. Anderson, "Why cryptosystems fail," in Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993, pp. 215–227.

[5] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens." WOOT, vol. 10, pp. 1–7, 2010.

[6] A. Oliva, A. Torralba, and P. G. Schyns, "Hybrid images," ACM Transactions on Graphics (TOG), vol. 25, no. 3, pp. 527–532, 2006.

[7] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010, pp. 1093–1102.

[8] L.-W. Chan, T.-T.Hu, J.-Y.Lin, Y.-P. Hung, and J. Hsu, "On top of tabletop: A virtual touch panel display," in Horizontal Interactive Human Computer Systems, 2008. TABLETOP 2008.3rd IEEE International Workshop on. IEEE, 2008, pp. 169–176.

[9] W. Matusik, C. Forlines, and H. Pfister, "Multiview user interfaces with an automultiscopic display," in Proceedings of the working conference on Advanced visual interfaces. ACM, 2008, pp. 363–366