Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

Realtime Eye Tracking for Password Authentication

Asha Rani K P[1], Asha K N[2], Nidhi B Channappagoudar[3], Manonandan S K[4]
Department of Computer Science and Engineering,
Dr. Ambedkar Institute of Technology,
Bengaluru-560056, Karnataka, India.

***Abstract* -- This paper focuses on entry of PIN using blinking method. Personal identification numbers are used for user authentication and security. Password verification using PINs requires users to enter a physical PIN, which can be vulnerable to password breakage or hacking via shoulder surfing or thermal tracking. PIN authentication with eye blinks entry techniques, does not leave any kind of physical footprints behind and therefore offer a more secure password entry option. Eye blinks-based authentication refers to finding the eye blinks across sequential image frames, and generating the PIN. This project presents a real-time application to avoid shoulder surfing and thermal tracking attacks.**

Keywords:- Python, Dlib , Secure authentication of PIN.

INTRODUCTION

Today, the Internet has entered into our day-to-day life and all the services have been moved online. Beyond reading the news, looking for information, and other threat free task, we have also become accustomed to other risk-related work, such as paying using credit cards, checking/composing emails, online banking, and so on. While we appreciate its benefits, we are placing ourselves at risk.

Eye tracking is the process of detecting the eye location across video frame. The motion of the eye relative to the head may also be more interest. Eye tracking is important for development and research areas such as visual systems, psychological analysis, cognitive science and product design. An eye tracking system is an integration of a set of devices and associated programs for measuring eye positions and movement, and correlating the results to the same eye across images acquired sequentially over time.

One of the security requirements for general terminal authentication systems is to be easy, fast and secure as people face authentication mechanisms every day and must authenticate themselves using conventional knowledge-based approaches like passwords. But these techniques are not safe because they are viewed by malicious observers who use surveillance techniques such as shoulder-surfing (observation user while typing the password through the keyboard) to capture user authentication data. Also, there are security problems due to poor interactions between systems and users. As a result, the researchers proposed a three-layered security framework to secure PIN numbers, where users can enter the password by blinking the eye at the suitable symbols in the appropriate order and thus the user is invulnerable to shoulder surfing. Eye blinking is a natural interaction method and security systems based on eye blink tracking provide a promising solution to the system security and usability. The aim of this paper is to review techniques or solutions to dealing with eye blink in security systems.

The use of personal identification numbers (PINs) is a common user authentication method for many applications, such a money management in automatic teller machines (ATMs), approving electronic transactions, unlocking personal devices, and opening doors. Authentication is always a challenge even when using PIN authentication, such as in financial systems and gateway management. According to European ATM Security, fraud attacks on ATM increased by 26% in 2016 compared to that of 2015. The fact that an authorized user must enter the code in open or public places make PIN entry vulnerable to password attacks, such as shoulder surfing as well as thermal tracking.

EXISTING SYSTEM

In current situation the methods of entering passwords are through hand, in terms of pin and passcodes, which as compared to latest technology are not enough safe. This statement considered to be correct because we have to think of that where current technology is heading and where are we in this trend. so as to compete with other systems we also should have enough sources for the same in this technological era as like providing safety to crucial workstations with certain system containing a strong password.

PROPOSED SYSTEM

The methods for entering passwords can be made safe enough using latest methods such as eye tracking. It means that make use of your eyes which will not leave prints like when we enter password by hands, which can be retrieved through silica gel, so there's no point of safe entry of password. So, the eye tracking system can be used for safer options which got many methods in it, here we choose is the method like blinking of eye for password authentication, which will not leave any prints behind.

LITERATURE SURVEY

Literature survey has been done on various systems. Empirical evaluation of the shoulder surfing phenomena is rare in password research to begin with. Most often, the concerns regarding shoulder surfing attacks are addressed in papers introducing novel graphical password authentication methods. To this day, it is common to find papers advertising a novel method as shoulder surfing resistant, though most of them do not explore that aspect beyond theoretical rationale (Li, Sun, Lian, Giusto, 2005, Shin, Kim, Hur, 2015, Yakovlev, Arkhipov, 2015). Some of them identify the investigation of the method's resistance as a plausible direction for future research (Lin et al., 2007), or even presume the method is safe against the attack by the virtue of its design.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

Zakaria et al. (2011) proposed three shoulder surfing defence techniques for the Draw A-Secret (DAS) recall-based graphical password scheme. In two separate experiments, susceptibility to shoulder surfing and usability were investigated. In the experiment of shoulder surfing, each participant was assigned one of the four experimental groups (three defence groups and a control group), and assumed the role of an attacker trying to steal three DAS passwords (weak, medium, and strong) during individual login attempts. The Real Time Eye Tracking Password Authentication results were organized into two groups based on the proportion of strokes shoulder surfed: DAS only, with Decoy Stroke defence had approximately 77% strokes guessed, while the Disappearing Stroke and Line Snaking defences had between 40% and 50% strokes guessed. The authors also reported the numbers of passwords completely, and partially stolen, as well as passwords completely resistant to shoulder surfing. The effect of password strength on the guessing success was also examined.

By this we declare that password authentication using the blinking method is the best technique to prevents from shoulder surfing, thermal attack or any other kind of attacks in present generation. This technology has more advantages than all the other which can be a threat to the user. This method is safe that users need not enter their PIN on the machine and it is easy to blink the digits and withdraw the amount.

ARCHITECTURE MODEL

The diagram shown below showcases the exact working of the password authentication model of the proposed system.
The execution initially starts with recognizing the face.
The detection of blinking and the analysis of blink duration are based solely on observation of the correlation scores generated by the tracking at the previous step using the online template of the user's eye. As the user's eye closes during the process of a blink, its similarity to the open eye template decreases. Likewise, it regains its similarity to the template as the blink ends and the user's eye becomes fully open again. This decrease and increase in similarity correspond directly to the correlation scores returned by the template matching procedure.

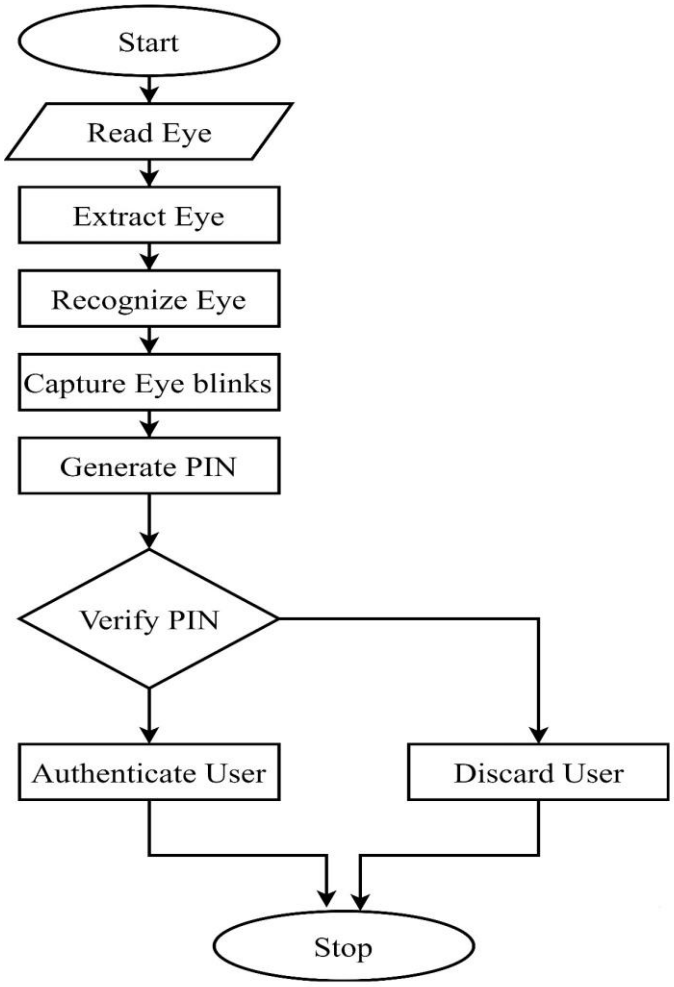

Figure 1: Architecture diagram of the Real Time Eye Tracking Password Authentication

The execution initially starts with recognizing the face. It captures eye position and recognizes the eye movement. When the user blinks the eye, it captures the eye blink. Finally, the PIN of the ATM. The PIN entered by the user will be verified by the system. If entered PIN is incorrect it will stop.

IMPLEMENTATION

By this we declare that password authentication using the blinking method is the best technique to prevents from shoulder surfing, thermal attack or any other kind of attacks in present generation. This technology has more advantages than all the other which can be a threat to the user. This method is safe that users need not enter their PIN on the machine and it is easy to blink the digits and withdraw the amount.

- First run the code.
- Three windows are displayed, one is virtual keyboard, another one is used to take input from user and the other is used to display the numbers selected by the user.
- In frame window the real time of the user is captured and their eyes are detected.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

- The digits displayed on the board windows is used to match that with the PIN.
- In virtual keyboard there are 10 digits (1,2,3,4,5,6,7,8,9,0), E(Enter) and P(Pop).
- The Pop key will pop the last selected number.
- The eyes will be surrounded by the red line when eye is open.
- Whenever the user blinks the eye, the color changes to green.
- Whenever the user blinks the eye, the color changes to number is selected and then we have to blink our eye for few seconds.
- Immediately taking the input the user will hear a beep sound then the user can open the eyes.
- After entering the password, if the password is matched then he/she will be recognized as an authenticated user else they must try for a second chance.

WORKING

Condition: Password Not Match

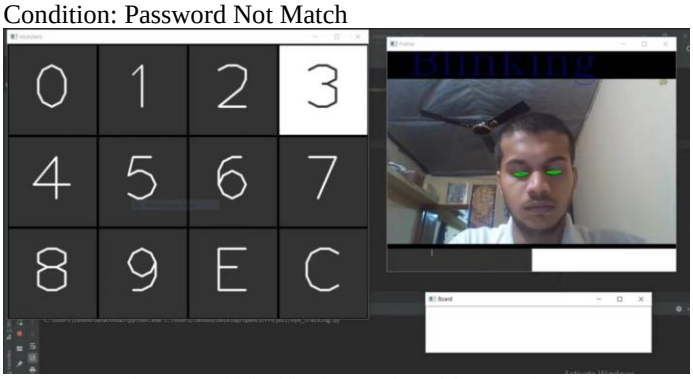

Figure 2.1: The personal identification number of the ATM is “26”. The user blinks the eye on number “3”, system takes the input “3” and then user blinks on ‘5”. The input will be “35”

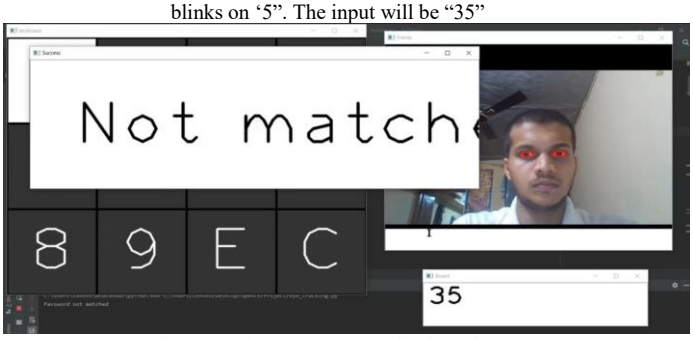

Figure 2.2: As the PIN is incorrect system displays the message “NOT MATCH”

Condition: Password Match

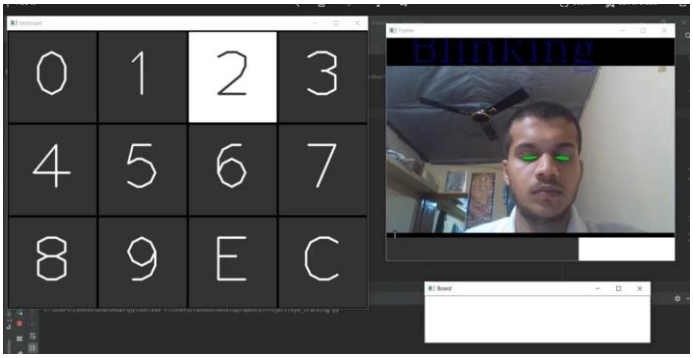

Figure 2.3: The user takes a next trial. The user blink the eye on number “2” and then will blink on “6” and blink on E(Enter)

Figure 2.4: As the PIN is “26”, the system displays the message “MATCHED”

RESULT

The large volume of data was conducted in order to access system accuracy and all the cases were successful. The implemented model is as shown in above figure Fig.2. The figure shows the complete implementation of the project. The password can be authenticated without the manual entry of the PIN. This method avoids Shoulder-Surfing, Thermal Hacking and many other which can be a threat to the user. This is the safe method to authenticate the PIN. The following figure shows the comparison between previously implemented method (gaze based) and our new method (blinking).

	Using eye gaze detection	**Using eye blink**
Accuracy	Low accurate	High accurate
Accessibility	Someone with eye problem will face difficult	Everyone can use easily
Time	Less time to authenticate	Little time consuming
Cost	Expensive	Cost Efficient
Implementation	Difficult	Easy

The comparisons clearly show that password authentication using blinking method is more efficient than the other method. The number of cases were experimented on this model using the conditions: “PASSWORD MATCH” and “PASSWORD NOT MATCH” any some more in which all the cases were 100% accurate. This is the new method that has not implemented earlier and this method is more secure than the physical entry of PIN which causes threats like shoulder-surfing, thermal hacking etc.

CONCLUSION

The main drawback like forgetting your passwords and leakage of the same can be overcome by this method and it is very safest option for the same. Usage of this technology will be helpful for each and every sector of this corporate world. Applications of this method can be used further for high end security systems by making some more improvements and research at higher level In all of the experiments in which the subjects were seated between 1 and 2 feet from the camera, it never took more than three involuntary blinks by the user before the eyes were located successfully. Another improvement is this system’s compatibility with inexpensive USB cameras, as opposed to the high-resolution colour video CCD camera. These Logitech USB cameras are more

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

affordable and portable, and perhaps most importantly, support a higher real-time frame rate of 30 frames per second. The reliability of the system has been shown with the high accuracy results reported in the previous section. The experiments indicate that the system performs really well in extreme lighting conditions (i.e. when all lights turned off, leaving the computer monitor as the only light source, and with a lamp aimed directly at the video camera). The accuracy percentages in these cases were approximately the same as those that were retrieved in normal lighting conditions.

REFERENCES

[1] 2018 IEEE International Conference on Consumer Electronics, Mr Kaustubh.S.Sawant, Mr. Pange P.D has published "Real-time eye tracking for password authentication using gaze based".
[2] M. Mehrubeoglu, H. T. Bui and L. McLauchlan, "Real-time iris tracking with a smart camera," Proc. SPIE 7871, 787104, 2011.
[3] M. Mehrubeoglu, L. M. Pham, H. T. Le, M. Ramchander, and D. Ryu, "Real-time eye tracking using a smart camera," Proc. 2011 IEEE Applied Imagery Pattern Recognition Workshop (AIPR '11), pp. 1-7, 2011.
[4] M. Mehrubeoglu, E. Ortlieb, L. McLauchlan, L. M. Pham, "Capturing reading patterns through a real-time smart camera iris tracking system," Proc. SPIE, vol. 8437, id. 843705, 2012.
[5] R. Revathy and R. Bama, "Advanced Safe PIN-Entry Against Human ShoulderSurfing," IOSR Journal of Computer Engineering, vol 17, issue 4, ver. II, pp. 9-15, JulyAug. 2015.
[6] J. Weaver, K. Mock and B. Hoanca, "Gaze-Based Password Authentication through Automatic Clustering of Gaze Points," Proc. 2011 IEEE Conf. on Systems, Man and Cybernetics, Oct.2011.
[7] "ATM Fraud, ATM Black Box Attacks Spread Across Europe", European ATM Security Team (E.A.S.T.), online, posted 11 April 2017.
[8] Smart Cameras for Embedded Machine Vision, (product information) National Instruments.