International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Eye Tracking for Password Authentication using Machine Learning

Mala B M[1], Pavithra A[2], Ranjeetha J[3], Yamuna R[4] & Smt. Manikantha K[5]

[1-4] Student BNMIT, Department of Computer Science & Engineering,
[5]Assistant Professor, Department of Computer Science & Engineering, BNMIT, Karnataka, India

---

Abstract – The personal identification numbers (PINs) is a common user authentication method for many applications, such as money transactions in automatic teller machines (ATMs), unlocking personal devices and opening doors. Authentication remains a challenge even when user enters a PIN in open or public places makes PIN entry vulnerable to password attacks such as shoulder surfing as well as thermal tracking. The use of PINs is especially true for banking applications where the combination of a token (e.g. bank card) and the user's secret PIN is commonly used to authenticate transactions. In financial applications PINs are typically four-digit numbers, resulting in 10000 possible numbers. The security of the system relies on the fact that an attacker is unlikely to guess the correct PIN number and that the systems (e.g., Automated Teller Machines) limit the user to few attempts (e.g., 3) for entering the correct PIN. To overcome shoulder surfing attacks, and enable users to enter their PIN without fear of being observed by developing a system that employs an eye tracking device. With safety PIN, users select PIN numbers with their eyes by simply focusing on the digits displayed on a screen. Gaze-based authentication refers to finding the eye location across sequential image frames. Haar Cascade algorithm is a machine learning approach which can be used for detecting the eye pupil location.

Key Words: Personal identification numbers (PINs), Eye centre, Pupil location, Gaze-based PIN entry, Haar Cascade.

1. INTRODUCTION

The use of PINs as passwords for authentication is ubiquitous nowadays. This is especially true for banking applications where the combination of a token (e.g. bank card) and the user's secret PIN is commonly used to authenticate transactions. In financial applications PINs are typically four-digit numbers, resulting in 10000 possible numbers. The security of the system relies on the fact that an attacker is unlikely to guess the correct PIN number and that the systems limit the user to few attempt for entering the correct PIN. As most applications that use PINs for authentication operate in a public setting a common attack is to try to observe and record a user's PIN entry (shoulder-surfing).

These security problems have been recognized for a long time and researchers have proposed a number of different schemes to minimize the risk of PIN entry observation. One such proposed alternate PIN entry method requires the user to input some information, which is derived from a combination of the actual PIN and some additional information displayed by the system, instead of the PIN itself. Another approach proposes the use of an elaborate hardware to make PIN entry resilient to the observation attacks. However, these methods have not been introduced into practical applications because the users would have to be retrained to use a completely different approach to PIN entry and the significant additional costs involved in the hardware setup.

Interaction with computers is not limited to keyboards and printers anymore. Different kinds of pointing devices, touch-sensitive surfaces, high-resolution displays, microphones and speakers are normal devices for computer interaction nowadays. There are new modalities for computer interaction like speech interaction, input by gestures or by tangible objects with sensors. A further input modality is eye gaze which nowadays finds its application in accessibility systems. Such systems typically use eye gaze as the sole input, but outside the field of accessibility eye gaze can be combined with any other input modality. Therefore, eye gaze could serve as an interaction method beyond the field of accessibility. 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 eye tracking systems, where users can enter the password by looking at the suitable symbols in the appropriate order and thus the user is invulnerable to shoulder surfing. Eye tracking is a natural interaction method and security systems based on eye movement tracking provide a promising solution to the system security and usability.

Some people interact with the computer all day long, for their work and in their leisure time. As most interaction is done with keyboard and mouse, both using hands, some people suffer from overstressing particulars parts of their hands, typically causing a carpal tunnel syndrome. With a vision of ubiquitous computing, the amount of interaction with computers will increase the need of interaction

techniques which do not cause physical problems. The eyes are a good candidate because they move anyway when interacting with computers. Using the information lying in the eye movements could save some interaction, in particular hand-based interaction.

The paper describes the following sections:

Section II gives the general methods for eye tracking. Section III gives the methodology. Section IV gives the proposed model. Section V gives the results. Section VI gives the conclusion.

2. Methods Influencing Authentication Mechanism of Eye Tracking.

The study of existing security systems that are based on eye movement tracking developed by different researchers according to their area of expert. In the following paragraphs are given several of the published researches related to the goals of this work.

A. Pin-entry against Human Shoulder-Surfing:

In computer security, shoulder surfing refers to using direct inspection techniques, such as peeping over someone's shoulder, to acquire information. Shoulder surfing is frequently used to acquire passwords, PIN security codes and related data. To stop shoulder surfing, which is between the customer and the system, cryptographic prevention approach is hardly relevant because users are restricted in their capacity to process information. Among them, the PIN entry technique introduced was effective because of its clarity and instinctive in every round, a structured numeric keypad is colored at odd half of the keys are in black and another half in white, which is called as BW method. A customer who knows the accurate PIN digit can enter the color by pressing the distinct color key below. The primary BW method is targeted to withstand a human shoulder surfing attack. [1]

B. Gaze-Touch Pass Scheme:

With mobile devices enabling ubiquitous access to sensitive information, there is a need to protect access to such devices. Meanwhile, authentication schemes are prone to shoulder surfing attacks, where a bystander observes a user while authenticating. The attacker then gets hold of the device and tries to authenticate and access sensitive data. To overcome this attacks Gaze Touch Pass, a multimodal authentication scheme in which user define four symbols, each can be entered either via touch (a digits between 0 and 9) or via gaze (gazing to the left and to the right). Consecutive gaze inputs to the same direction would then need to be separated by a gaze to the front and switches between input modalities are used within a single password. [2]

C. Eye Gaze Classification for iTyping :

Human emotions and cognitive states are essential in developing a natural human-computer interaction system (HCI). Systems which can identify the affective and cognitive states of humans can make the interaction more natural. The knowledge of mental processes can help computer systems to interact intelligently with humans. Estimation eye gaze direction is useful in various human-computer interaction tasks. Knowledge of gaze direction can give valuable information regarding user's point of attention. A real time framework which can detect eye gaze direction using low-cost cameras in desktops and other smart devices. Estimation of gaze location from webcam often requires cumbersome calibration procedure. Gaze direction classification as a multi-class classification problem, avoiding the need for calibration. The eye directions obtained can be used to find the EAC and thereby infer the user's cognitive process. The information obtained can be useful in the analysis of interrogation videos, human-computer interaction, information retrieval, etc.

D. To Enhance iTyping Privacy:

Mobile devices offers the most convenient user experience ever, e.g., at anytime and anywhere, but users unavoidably face a new potential threat at the same time. The interaction between users and mobile devices may be exposed to public directly, which may leak very sensitive information of the user, e.g., passwords, private data, account information, etc. If the input of such information is not properly protected, the user's privacy can be easily emanated and compromised in public. iTyping is for entering the private information using the eye gaze. In iType, the keyboard consists of multiple buttons and each button represents unique character(s) (number or letter). For the ease of presentation, it refers password to various kinds of private information for short. To type a password, the user looks at the corresponding buttons sequentially and iType essentially solves a decoding puzzle it reads the user's gaze, infers the buttons being looked at and assembles the password. The iTyping is secure primarily due to the fact that the eye gaze is difficult to eavesdrop. Even an adversary in front of the user could decode the eye gaze, the gaze itself conveys no meaningful information, unless it matches with the keyboard layout, which however can be user-defined and changed. [4]

E. Accuracy and Precision of Eye Tracking:

To establish eye gaze as part of everyday interaction with computers, it needs to understand the characteristics and limitations of eye tracking in practice and derive standards for the design of gaze-enabled applications that take into account that accuracy and precision can vary widely across different tracking conditions. It collects calibration style eye tracking data from 80 participants, using two different

trackers in two lighting conditions. In contrast to many eye tracking studies, It does not exclude any participant due to insufficient tracking quality and only calibrated once at the beginning. Finding a several contributions for the design and development of gaze-enabled applications.

1. Checking the accuracy and precision ranges overall and for different parts of the screen that characterize the large variation across different tracking conditions.

2. Provides a formal way to derive appropriate target sizes from measures of accuracy and precision. Based on data user gives a recommendation for the minimum size of gaze-aware regions to allow robust interaction.

3. An approach to find optimal parameters for any filter that minimizes target size and signal delay. [5]

To overcome all the above issues by implementing a real time hands-off gaze-based PIN entry technique is used, which leaves no footprints. Gaze-based authentication refers to finding the eye location across sequential image frames and tracking eye centre. Haar Cascade algorithm is a machine learning approach used for detecting the eye pupil location by Image Processing. In this technique, several stages are used to find out the movement of eye, such as Face detection and Eye detection, Edge detection. The distance between the centre point and eye pupil centre are measured using coordinates system logic. According to the eye pupil movements, the measured distance will vary.

A minimum distance indicates the eye pupil is moved towards the left, and maximum values indicates the eye moved on right and if there is no movements of the eye, then it concludes that eye is in the middle position. After tracking the eye pupil position, the data is taken by the system. The entered data is compared with the trained dataset. If the entered data is not matched with the trained data then the system will throw an error as "unauthorized access" else the system confirms and allows for further transaction.

3. METHODOLOGY

Firstly, user has to scan the RFID card to generate OTP which serves as a password. Once OTP is generated camera module starts to capture the images. For the face detection, Haar cascade algorithm is used. After the detection of the face, the algorithm will try to detect the eye on the face, which is a region of interest. The system will corp the eye region initially and it will detect the eye center point. Corner detection method is applied to find out the regions of eye corners. The distance between the eye region corner and eye pupil center are measured using coordinates system logic. With safety PIN, users select PIN numbers with their eyes by simply focusing on the digits displayed on a screen, then entered PIN is compared with generated PIN. If the entered PIN is not matched with the trained data then the system will display an error message as "Password not matched" else the system confirms and allows for further transaction.

4. PROPOSED MODEL

Eye-driven computer operation requires certain steps of processing of an image captured with a web camera. The following figure 1 presents the general scheme of the process.

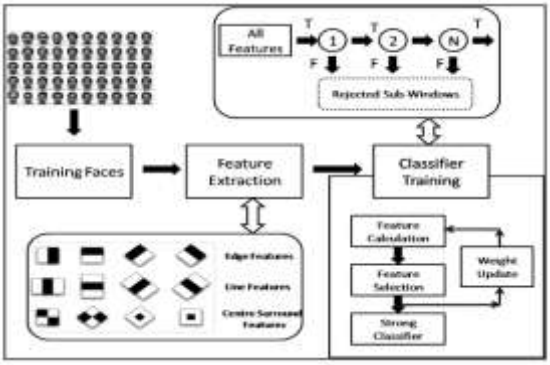


Fig-1 System design of Eye tracking System.

4.1 Web camera

A webcam is a video camera that feeds or streams its image in real time to or through a computer to a computer network When "captured" by the computer, the video stream may be saved, viewed or sent on to other networks travelling through systems such as the internet, and e-mailed as an attachment. When sent to a remote location, the video stream may be saved, viewed or on sent there. Unlike an IP camera (which connects using Ethernet or Wi-Fi), a webcam is generally connected by a USB cable, or similar cable, or built into computer hardware, such as laptops.

4.2. Eye detection

Eye will be detected from the images that are captured from the web camera and Haar cascade algorithm is used to detect the eye.

4.3. Feature detection

Feature detection takes input from the eye detection module as a Haar classifier to locate the coordinate points for the eye pupil position, then gaze values will be calculated.

4.4.Eye tracking

Eye blink ratio is calculated and the corresponding number from the keyboard is updated as pin and sent for further authentication process.

4.5. RFID reader

RFID uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy

from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method of automatic identification and data capture (AIDC).

5. RESULTS

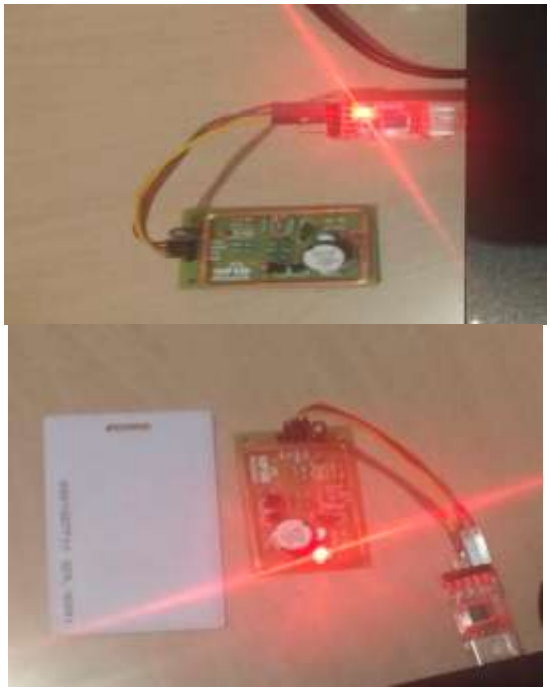


Fig-2 RFID reader and RFID card

Fig 2 shows the hardware component of RFID reader and card. RFID is used to scan the card to generate OTP.

Fig-3 Generating OTP.

Fig 3 showing the result of generating of OTP. In this user scans a RFID card through RFID reader to get OTP for the specific card.

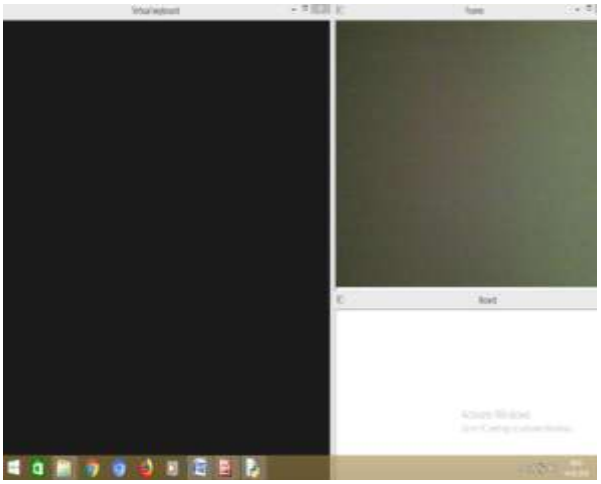


Fig-4 Virtual keypad is not displayed on the screen.

Fig 4 showing the results of not displaying virtual keypad. In this user facial image is recognized through web cam, if the facial image is not recognized then virtual keypad is not displayed on the screen.

Fig-5 Facial image is recognized through web cam, then virtual keypad.

Fig 5 shows virtual keypad along with facial image. In this user facial image is recognized through web cam, then virtual keypad is displayed on the screen along with the frame where facial image is cropped with eye region denoted by red color. If user does not enter the pin with in a seconds terminal closes displaying time out.

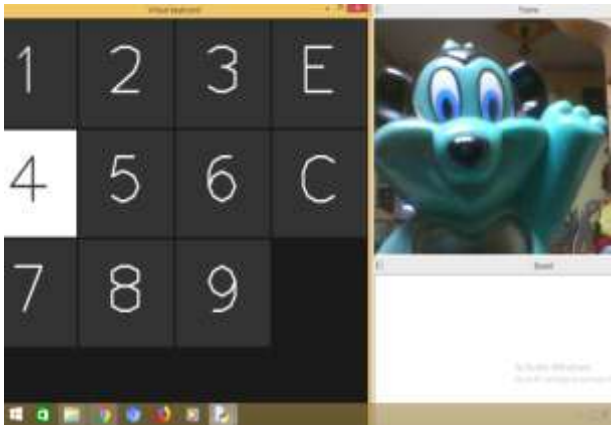
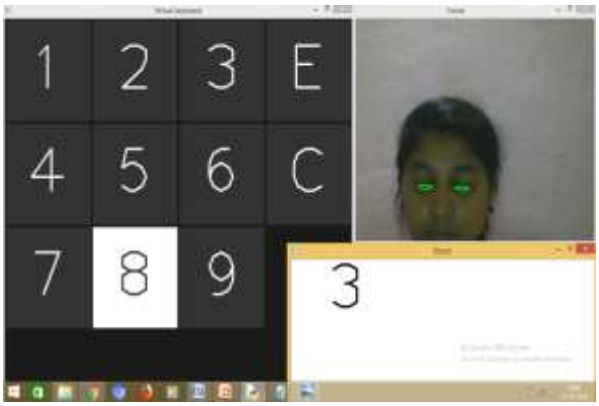


Fig-6 Image is not recognized by web camera

Fig 6 shows that camera detects object rather than human face it does not crop the eye region and it does not allow for further process.



Figu-7 Virtual keypad taking input through eyes.

Fig 7 shows virtual keypad along with facial image. In this user facial image is recognized through web cam, once the facial image is recognized then virtual keypad is displayed on the screen. If the eye movement is recognized by virtual keypad then the eye region denoted by green color to enter the pin.

Fig-8 Password Matching.

Fig 8 shows the results of matching password. User starts entering pin which was generated as OTP through eye movement if the entered pin matched with the generated pin then it displays as password matched.

Fig-9 Password Not Matched.

Fig 9 shows the results of matching password. User starts entering pin which was generated as OTP through eye movement if the entered pin matched with the generated pin then it displays as password not matched.

CONCLUSION

In order to protect the users from shoulder-surfing in ATMs while entering the PIN, new method of entering the PIN are being evaluated. With the eye interaction for PIN entry is emerging as a practical solution. Here we have discussed Safety PIN, which proposes retrofitting the ATMs with an eye tracking device, so that users can enter their PIN without using keypad for pin entry. In addition to look and shoot and gaze activation methods, by introducing a new activation method called blink activation. Real time implementation of the algorithm has been done. The detection rate of the algorithm is well above the required accuracy rate. The speed of computation is more than the requirements needed. Only a small set of Haar like features are used to detect the face in real time. The Haar classifier based algorithm for face detection was found to be working with accuracy of 72%. Initial user evaluations have yielded encouraging results, prompting further work.

References

[1]. R. Revathy and R. Bama, "Advanced Safe PIN-Entry Against Human Shoulder Surfing," IOSR Journal of Computer Engineering, vol 17, issue 4, ver.II, pp. 9-15,July,Aug.2015. (http://www.iosrjournals.org/iosrjce/papers/Vol17issue4/Version2/B017420915.pdf).

[2]. Mohamed, Florian, Mariam, Emanuel, Regina and Andreas "Gaze-Touch Pass Scheme", March 2016.

[3]. Anjith George, Aurobinda Routray "Real time Eye Gaze Direction Classification Using Convolutional Neural Network", June2016.

[4]. Zhenjiang Li1, Mo L, Prasant Mohapatra, Jinsong Han, Shuaiyu Chen "iType Using Eye Gaze to Enhance Typing Privacy", 2017.

[5]. Puja sorate, Prof. Mrs. G. J. Chhajed "Survey Paper on Eye Gaze Tracking Methods and Techniques", International Research Journal of Engineering and Technology (IRJET) e-ISSN.