Gaze PIN Entry for Password Authentication

[1]Mr.RaghavendracharS, [2]SoumyaDattatreyaHegde, [3]VarshaPurushotham, [4]VennalaKN, [3]VidyashreeS,
[1]Assistant Professor, [2,3,4,5] Student
[1, 2,3,4,5] Department of Computer Science and Engineering,
[1, 2,3,4,5] K.S.Institute of Technology, Visvesvaraya Technological University, Karnataka, India

Abstract : Personal identification numbers are widely used for user authentication and security. Password authentication using PINs requires users to physically input the PIN, which could be vulnerable to password cracking via shoulder surfing or thermal tracking. PIN authentication with hands-free gaze based (by closing the eye) PIN entry techniques, on the other hand, leaves no physical marks behind and therefore offer a more secure password entry option. Gaze-based authentication refers to finding the eye location across consecutive image frames, and tracking eye center over time. This paper presents a real-time application for gaze-based PIN entry, and eye detection and tracking for PIN identification using a smart camera.

IndexTerms **- Gaze based PIN Entry, Security, Eye tracking, Eye blinking.**

I. INTRODUCTION

The use of PINs is a common method for many application, such as unlocking secret devices, locking and unlocking of doors and for other banking services. According to statistics about 51,000 people were victims of personal data breaches and 16,000 were victims of identity theft scams and accounted 57 percent of all losses in 2018.It is because that an legitimate user entering the code in open and public areas. This makes PIN entry being attacked such as phishing attack and thermal tracking. The main purpose of this work is to enter and identify gaze based PINs using a smart camera through real-time eye detection and tracking. Detection of eye and tracking of eye is done under different conditions, including angles of the face, head movement, location of eye in the face and the state of the eye whether it is closed or open to determine the usability of the system for real-time applications. We make use of Python OpenCv for eye tracking and for recording the state of the eye. Smart Camera allows on board data processing and collection. This type of authentication adds a layer of security to physical entry and expected to reduce the vulnerability of the authentication process.

II. LITERATURE REVIEW

The important problem in information security is user authentication. There are many authentication techniques are textual, graphical or biometric passwords etc. The text based password is easily guessed by the attacker over to nearby shoulder; attackers observed directly or watch some external devices. The text based password authentication methods are not enough for shoulder surfing attacks. The graphical based password authentication is best, because it is more secure and it provides better resistance to shoulder surfing attacks. The traditional two-factor authentication mechanisms aren't applicable to online social networks, because the physical token or biometric information can't be simply accustomed login to users' profiles.

Shoulder surfing enables an attacker to understand the authentication details of a victim through observations and is becoming a risk to visual privacy. The author [2] present DyGazePass: Dynamic Gaze Passwords, an authentication strategy that uses dynamic gaze gestures. We also present two authentication interfaces, a dynamic and a static-dynamic interface, that support this strategy to counter shoulder surfing attacks. The core idea is, a user authenticates by following uniquely colored circles that move along random paths on the screen. The author [3] presents SAFE (Secure Authentication with Face and Eyes) an improved face authentication method that uses a commodity gaze tracker to input a secret. During authentication, the user must not only show her face but also looked at a secret icon that moves across the screen. Using a novel method for estimating the background level within the gaze tracking data, SAFE adapts the system's parameters to enable secure, hands-free authentication.

Real-time eye detection and tracking [4] have been developed not for a PC but for use in a standalone smart camera with DSP capabilities. The tracking algorithm is enhanced and simplified for the NI Smart Camera. The paper [5] presents an eye fixed fixed tracking study of Image Pass, a recognition-based graphical authentication mechanism. The goal of the study was to discover how users perceive and react to graphical authentication. The author [6] describe the EyeDent system—in which users authenticate by looking at the symbols on an on-screen keyboard to enter their password. Instead, in EyeDent, gaze points are automatically gathered to work out the user's selected symbols; this approach has the advantage of allowing users to authenticate at their natural speed, rather than with a fixed dwell time.

Click-based graphical passwords are a replacement method of authentication where passwords are created and entered by clicking especially places on a picture. This paper presents [7] a study that investigated eye tracking as a potential threat to the security of such passwords. A simple biometric based on a gaze sequence on a personal computer screen has been described [8]. The experiments reported above have validated the suitable performance of the approach and demonstrated that it's comparable conventional PIN based user authentication.

III. SYSTEM DESIGN AND ARCHITECTURE

The camera is allowed to capture the images. The first direction is to detect the user Face accurately.In this technique several stages used to find out the movement of eye, such as Face detection and Eye detection, colour conversion, Edge detection, Hough Transformed, motion detection and eye tracking.After that system will perform the several operation of image processing to track the eye pupil. For the detection of face Haar cascade algorithm is used. Haar cascade classifier is used to calculate the position of eye gaze based on features of human eye. For detecting pupil area Hough transform method is used. Virtual keypad will be displayed on the screen.

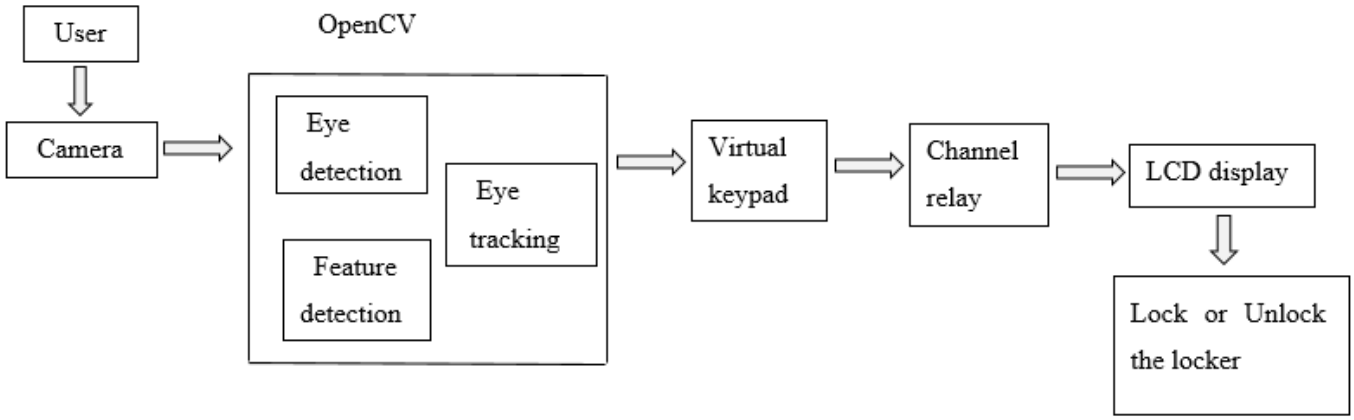

Figure 1: Block diagram of proposed system

3.1 Camera

Web camera is used to capture the continuous images i.e., the video of the person in front of the camera. The captured image acts as input to OpenCV. This captured image is sent Eye detection module.

3.2 OpenCV

The image from the camera is fed into OpenCV. This image is sent to eye detection module in OpenCV where the face and eye region in the image would be captured and the respective window location is sent to feature detection module, here the co-ordinates of the eye region is will be the output. Lastly in the eye tracking module the eye movements will be tracked to get the gaze ratio and the eye blinks will be detected to get the blinking ratio. Based on these two ratios the password would be updated.

3.3 Channel Relay

Relay is a system which needs password to open. Once after the authentication process is completed the relay system is made opened. If the authentication is success then the relay system is opened else if the authentication process is failed then the relay system remains closed.

3.4 LCD Display

LCD display is used for displaying password match or mismatch.

IV. IMPLEMENTATION

4.1 Eye Detection

Eye detection module is used to detect the eye region in the given image. Haar cascade algorithm is used to achieve the task. Haar cascade algorithm is the machine learning object detection algorithm used to identify objects in an image or video based on the concept of features.OpenCV will help in detecting the eye.

4.2 Eye Tracking

In this module continuously the eye movement is tracked to obtain the Gaze Ratio and based on the gaze ratio the respective keyboard will be displayed. Then the eye blinking ratio will be calculated to update the respective letter as the password. The algorithms for implementing eye tracking is given below.

Algorithm 1: *To calculate the gaze ratio*

1. Input the pixel values of the eye region.
2. Get only the eye region
3. Divide each eye region into left and right part
4. Convert the eye image into grayscale
5. Get the number of white pixels on both side i.e., on the left side and right side of each eye.
6. Calculate the gaze ratio.

   If Gaze Ratio <= 0.9 then select the right keyboard

   Else

   then select the left keyboard.

Algorithm: To calculate the Blinking Ratio

1. Input is the co-ordinate values of the eye region
2. Obtain the horizontal and vertical of left eye :
   i. Calculate the midpoint of 37^{th}, 38^{th} co-ordinate and 40^{th}, 41^{st}coordinate.
   ii. Join the points to the vertical line.
   iii. Join the 36^{th} and 39^{th} point to get the horizontal line.

3. Obtain the horizontal and vertical of righteye:
   i. Calculate the midpoint of 43^{rd}, 44^{th} co-ordinate and 45^{th}, 46^{th}coordinate.
   ii. Join the points to the vertical line.
   iii. Join the 42^{th} and 47^{th} point to get the horizontal line.

3. Calculate the Blinking Ratio :
4. Initialize the Blinking frames to zero
5. If Blinking ratio >=5
   Increase the blinking frames value by one
   Else
      Do nothing
6. If Blinking frames ==6

      Then update the letter as password

When the user blinks the eyes for given password the particular letter is selected shown in Figure 2.

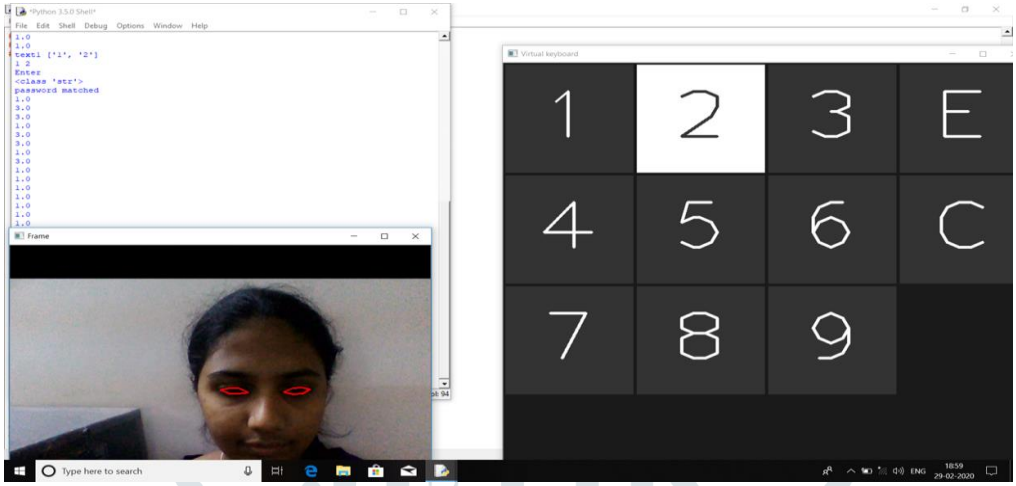

Figure 2: Password match after entering correct PIN

When the password selected is correct, password match message will be displayed on the LCD display and the user will get a message as VALID PASSWORD and hence the lock will open. Otherwise, password not matched is displayed and user will get a message as INVALID PASSWORD through telegram application and lock does not open.

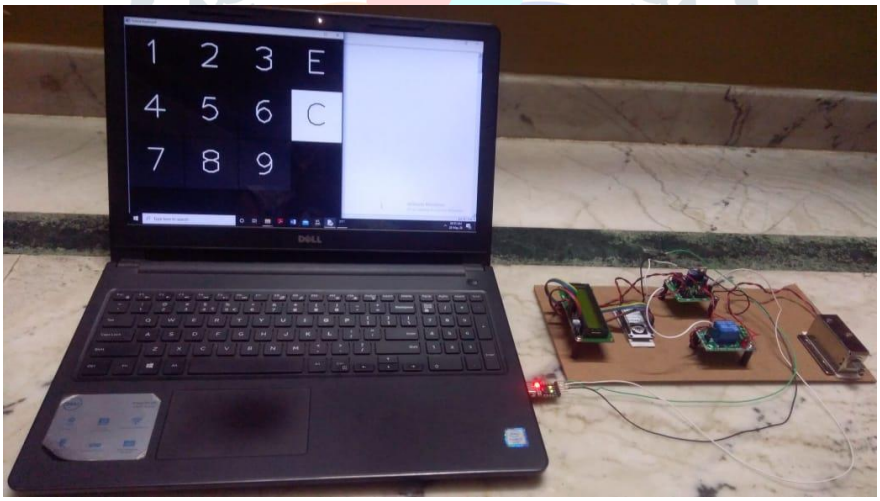

Figure 3: Snapshot of proposed system along with hardware

When password matches or mismatches the user will get the message through telegram app showing VALID or INVALID PASSWORD which is connected through the user's Wi-Fi to the NodeMCU as shown in Figure 4.

Figure 4: Telegram app showing VALID or INVALID messages.

V. CONCLUSION AND FUTUREWORK

A smart-camera based eye-tracking system has been incorporated as a new application for gaze-based PIN identification. The system has been successfully tested with numbers, and can be extended to character and digit combination password entry. This system mainly protects the user password from various attacks like shoulder surfing and thermal tracking and it is also helpful for the physically disabled persons who are not able to enter password manually. The stability of the user's gaze will affect the accuracy of the detected pins, and must be accounted for. Currently, the PIN identification is accomplished after real-time eye tracking and eye Centre computations and recording are completed. Future enhancements includes incorporating the PIN identification algorithm into the-real-time framework for all in one password identification system. Gaze-based password entry can be extended to mobile devices and other camera-based systems.

REFERENCES

[1] Vijay Rajanna ; Adil Hamid Malla ; Rahul Ashok Bhagat" A gaze gesture-based dynamic authentication system to counter shoulder surfing and video analysis attacks" 2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)

[2] Marco Porta ; Alessandro Barboni "Strengthening Security in Industrial Settings: A Study on Gaze-Based Biometrics through Free Observation of Static Images"2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)

[3] A. Maeder ; C. Fookes ; S. Sridharan "Gaze-based user authentication for personal computer applications" Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004.

[4] Arman Boehm ; Dongqu Chen ; Mario Frank ; Ling Huang ; CynthiaKuo ; TihomirLolic ; IvanMartinovic ; Da wn Song "SAFE: Secure authentication with Face and Eyes " 2013 International Conference on Privacy and Security in Mobile Systems (PRISMS)

[5] Justin Weaver ; Kenrick Mock ; Bogdan Hoanca **"**Gazebased password authentication through automatic clustering of gaze points**"** 2011 IEEE International Conference on Systems, Man, and Cybernetics

[6] Daniel LeBlanc ; Alain Forget ; Robert Biddle "Guessing click-based graphical passwords by eye tracking" 2010 Eighth International Conference on Privacy, Security and Trust

[7] Mehrube Mehrubeoglu ; Linh Manh Pham ; Hung Thieu Le ; Ramchander Muddu ; Dongseok Ryu "Real-time eye tracking using a smart camera"2011 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)

[8] Mihajlov Martin ; Trpkova Marija ; Arsenovski Sime "Eye tracking recognition-based graphical authentication" 2013 7th International Conference on Application of Information and Communication Technologies