

Password Authentication Using Gaze Based Eye Tracking

Srikanth M S¹, Dr Jitendranath Mungara², Monisha N³, Pramod C R⁴, Roopika T C⁵, Vinod B S⁶

¹Assistant Professor, Department of Information Science and Engineering, Nagarjuna College of Engineering and Technology, Bangalore, Karnataka, India

²Principal & Professor, Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, Bangalore, Karnataka, India

^{3, 4, 5, 6}B. E. Student, Department of Information Science and Engineering, Nagarjuna College of Engineering and Technology, Bangalore, Karnataka, India

ABSTRACT

Article Info

Volume 8, Issue 3

Page Number : 01-05

Publication Issue

May-June-2021

Article History

Accepted : 07 May 2021

Published : 14 May 2021

“Password Authentication Using Gaze Based Eye Tracking” is a system used for eye(retina) tracking using Haar cascade algorithm, Facial Landmark Algorithm. used for password authentication. A mounted camera will track eye movement and by eye movement and eye blinks it calculates gaze ratio and blinking ratio which are two mains to lock and unlock the system, this is aimed to make the system highly securable and to avoid cybercrimes like shoulder surfing or thermal tracking.

Keywords : - Haar cascade algorithm, Facial Landmark Algorithm.

I. INTRODUCTION

The modern world where we are today there are many new technologies which are updating day to day even second to second there are many advantages to the citizens. It has made all works easier even the work may be good or bad. So the security issues will be the foremost thing where we have to focus on, As we all are aware that PIN is mostly used authentication method for many applications, like for unlocking electronic gadgets, automatic teller machines (ATMs), for approving e-transactions, and even at home automation. When we come to the case of ATM machine in existing the user have to enter the personal identification number s(PINs) manually

and it may lead to cyber-crimes such as password attacks, shoulder surfing etc.

The aim of this system is to overcome the issues of the existing system and to make the system highly securable this can be achieved by techniques of Image Processing like Haar cascade algorithm, Facial Landmark Algorithm. Contact less PIN base authentication adds extra layer of security than physical PIN entries and are expected to reduce the vulnerability of the authentication process.

II. LITERATURE SURVEY

In the process of developing this system we have gone through many IEEE papers and Journal published papers. It helped us a lot in order to finish the work

and here is the list of the papers on which we surveyed and helped us in the completion of the system. Extension of desktop control to robot control by eye blinks using Support Vector Machine (SVM) is one of the papers by author Naga Soundari in the year 2011 and the work done in this paper are issues related to Accessibility, which should eliminate, or at least reduce, the distance between disabled people and technology. In other paper titled Eye movement-related EEG potential pattern recognition for real-time BMI by author Takuma Ito in the year 2010 This study aims at rapid BMI pattern recognition for the eye-ball movement, Since the system was based on the concepts of Image Processing even got an idea of using Haar cascade technique detecting the movement of the eye and calculating it. Next the paper titled Quantitative analysis of tennis experts' eye movement skill by author Sota shimiju in the year 2014. In this study, eye movements measured from 2 categories, i. e. , tennis experts and beginners are compared and analysed as regarding eye movement as a kind of motion skills. In our work we done using 68 facial landmark algorithm we are tracking the eye points from the face. We will consider the eye movements will tracked to get the gaze ratio and the eye blinks will be detected to get the blinking ratio. At last, a paper titled Smart eye-tracking system by the author Aniwat in the year 2018. In this paper we learnt about the technology and methods used for eye tracking for disabled people.

III. SYSTEM REQUIREMENTS

3. 1 Software specifications:

- **Operating system:** Windows XP/ Windows 7/8/10.
- **Software Tool:** Open CV Python
- **Coding Language:** Python
- **Toolbox:** Image processing toolbox.
- Twilio account

3. 2 Hardware specifications:

- **Hard Disk:** 500 GB.
- **RAM:** 4 GB or more
- **Processor:** Intel i3 and above

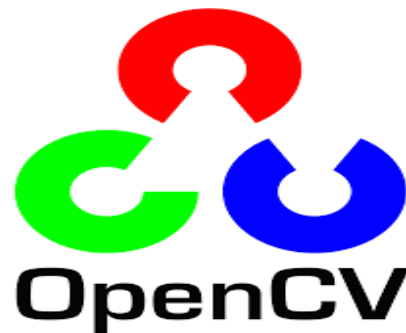
1. Python:

Python 2. 7. 13. Python is a dynamic object-oriented programming language that can be used for many kinds of software development.



2. Open CV:

Open CV (OpenSource Computer Vision Library) is an open source computer vision and machine learning software library.



IV. SYSTEM ANALYSIS

4. 1 Existing System:

In current situation the methods of entering passwords are by hand, in terms of pin and passcodes. These methods for latest technology are not enough safe. In user authentication, all user can do is providing user credentials i. e. , username and password. Generally, password systems face many problems of conflicting requirements. The passwords that user provides must be user friendly. The next requirement is that the passwords should be secured.

Since the existing system is not highly secured, it may lead to several Cyber-crimes.

4. 1. 1 Disadvantages

- Keypad based systems which are very to hack.
- Voice Controlled password which is user specific.
- Head controlled or gesture-controlled systems where physical movement is required, which will be inconvenient to user.
- Most of them are sensor dependent systems which will be inaccurate.

4. 2 Proposed System:

Our project is an eye blink-based password entry. The mounted camera will track eye Blink and check the authentication. The first part is the head mounted camera that will track the camera wearer’s eyes using PC with Open cv. The pc will take a USB output from the camera and convert the signal into digital signals. If the user is known it will allow the user to enter the password using virtual keyboard on blinking the eyes. If the user is unknown a message is sent to the owner as “Unknown person detected”.

4. 2. 1 Methodology

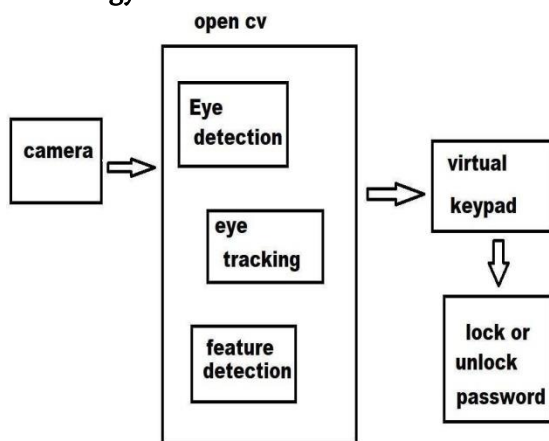


Fig 1. Architecture diagram

The above-mentioned image will show the complete methodology process of proposed implementation. First module is camera, it is used to capture the images of the user and it will be used for face and eye detection. Open CV is used to identify the particular

regions in the face captured by camera. It includes three modules eye detection, eye tracking, feature detection. Image that is captured from the camera is sent to eye detection module where the **Haar cascade algorithm** is used to detect the face in the image and in that face region the eye region will be detected. The specific window location is sent to next module.

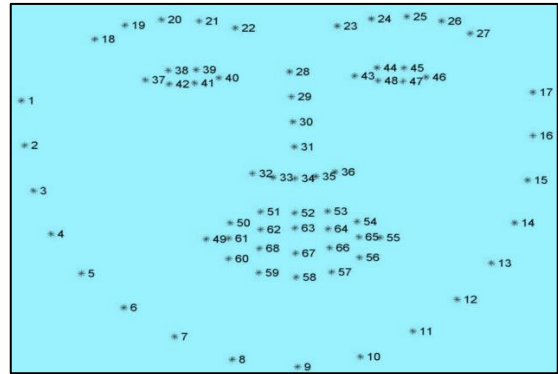


Fig 2. 68 Facial landmark points

In face detection we use the algorithm 68 facial landmark points, here we concentrate on the eye region points of both eyes are used to track the eye. Then we calculate the gaze ratio of both eyes for password authentication. It will draw a polygon around the eye region using this algorithm.



Fig 3. polygon drawn around the eye

First the user should capture his images, the virtual window will be opened to capture the images, it will take 50 images of the user within few seconds. And is stored in a folder. After that the user should click on eye tracking, if the user is authorized it will detect the user id and virtual keyboard is opened for entering the password. The user should blink his eyes accordingly to enter the password, if it matches it will display like password matched or else password unmatched. If the user is not authorized it will send a message to the owner as Unknown person detected. This is done using Twilio account.

4. 2. 2 Advantages

- Provides high Security
- Power consumption is less
- Accurate
- Real-time system
- Easy to implement
- It is portable device with Low cost
- Used commonly available components.

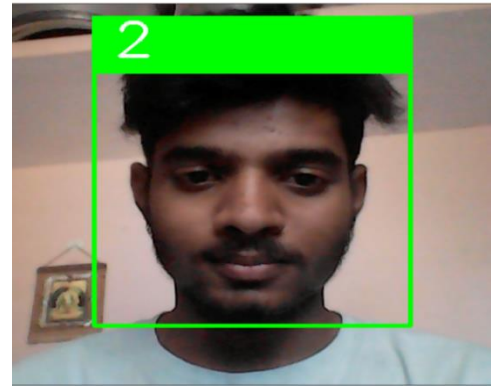


Fig 3 : Face capturing screen

V. RESULTS

We have used one use interface screen for this work. There are four buttons: face Capturing, Training faceid, Face Recognition & password detection, and Quit.

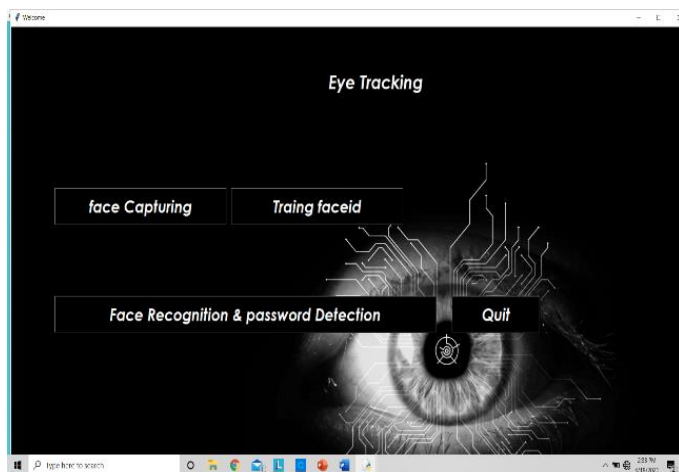


Fig 4 : User interface for eye tracking

Face capturing: On clicking this button the virtual window is opened where the user pictures are captured. 50 images are captured within few seconds and is converted into gray image and is stored in folder.

Face recognition & password detection: On clicking this button the virtual window is opened where user image is tracked and verified and then the virtual keyboard is opened to enter the password.

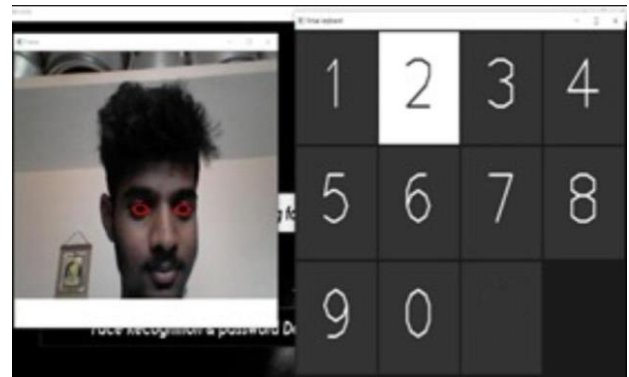


Fig 5. When eyes are open (Red color)

When user is detected the virtual keyboard will open as shown in the figure. User should keep his eyes open until the first number of password arrives. The red color polygon is drawn when eyes are kept open.

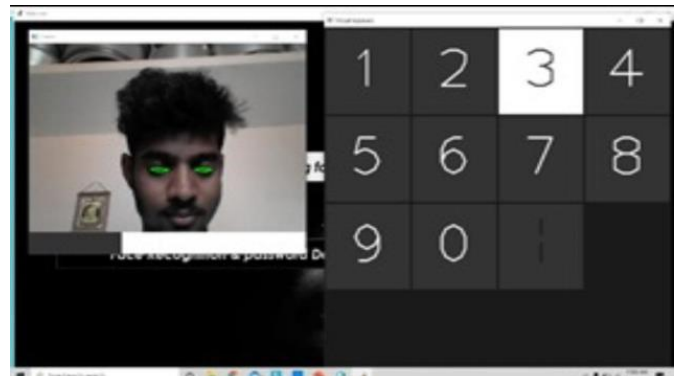


Fig 6: When eyes are closed (Green color)

Assume password is "34", then user should close his eyes when 3 is arrived in keyboard. At that time the polygon drawn around the eyes changes to green color. The user should close the eyes for some time,

then the number 3 will be selected as first letter of password, and in the same way 4 should be selected. Then it will give you a voice message as Password matched and in output screen also it displays a message as Password matched.

If password is not correct, then it gives a message as password unmatched. If unknown person is detected a message is sent to the owner.

VI. CONCLUSION

A "Password Authentication Using Gaze Based Eye Tracking" is a new application used for PIN entry, where eye tracking technique is used to unlock the password. The user can protect 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.

Future implementation can be done by extending the number keyboard to character keyboard so it provides more security. And this can be implemented in all camera-based devices.

VII. REFERENCES

- [1]. Sarangi, P., Grassi, V., Kumar, V., Okamoto, J.: "Integrating Human Input with autonomous behaviours on an Intelligent Wheelchair Platform", *Journal of IEEE Intelligent System*, 22, 2, 33-41, [2007].
- [2]. Matt Bailey, ET. Al, "Development of Vision Based Navigation for a Robotic Wheelchair", in *Proceedings of 2007 IEEE 10th International conference on rehabilitation robotics*.
- [3]. Shafi. M, Chung. P. W. H.: "A Hybrid Method for Eyes Detection in Facial Images",
- [4]. https://www.researchgate.net/publication/318177511_Eye_Tracking_Graphical_Passwords
- [5]. <https://www.eecis.udel.edu/~hnw/paper/acns15> Exploiting Eye Tracking for Smartphone Authentication.
- [6]. K. Mowery, S. Meiklejohn and S. Savage, "Heat of the Moment: Characterizing the Efficacy of Thermal

- Camera-Based Attacks," *WOOT '11*, pp. 1-8, August2011
- [7]. L.McLauchlan,H.T.BuiandM.Mehrübeoglu,"Real time iris tracking with a smart camera," *Proc. SPIE 7871, 787104,2011*.
- [8]. L. M. Pham, M. Mehrubeoglu, H. T. Le, M. Ramchander, and D. Ryu, "Realtime eye tracking using a smart camera," *Proc. 2011 IEEE Applied Imagery Pattern Recognition Workshop*
- [9]. "Healthcare Solution based on Machine LearningApplications in IOT and Edge Computing" at *International Journal of Pure and Applied Mathematics,Volume 119,No 16, 1473-1484, ISSN: 1314-3395, 2018*
- [10]. "Edge Computing Applications on Vehicular Networks" at *IC-IREASM-2019, ISSN 2348-4918. VOL 06, SPECIAL ISSUE 06 October 2019*
- [11]. "A Review of Security Strategies used in Vehicular Adhoc Networks" *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 4, Issue 9, November-December 2019*
- [12]. EDGE COMPUTER-ENABLED INTERNET OF VEHICLE APPLICATIONS WITH SECURE COMPUTING AND LOAD BALANCING, Darpan Majumder, S Mohan Kumar, D V Ashoka, A ShajinNaragunam, *International Conference on Emerging Trends in Science, Engineering and Management VIRTUAL CONFERENCE (ICETSEM-2021), 21st - 23rd January 2021*
- [13]. A Review of Black and Gray Hole Attacks in AODV published in *First International Conference on Emerging Trends and Challenges in Applied Science, Engineering and Technology (ICECAET - 2020)"Organizing by Gopalan College of Engineering and Management, on 10th and 11th , March, 2020*

Cite this article as :

Srikanth M S, Dr Jitendranath Mungara, Monisha N, Pramod C R, Roopika T C, Vinod B S, "Password Authentication Using Gaze Based Eye Tracking", *International Journal of Scientific Research in Science and Technology (IJSRST)*, Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 3, pp. 188-192, May-June 2021. Journal URL : <https://ijsrst.com/IJSRST218352>