

# Gaze PIN entry for Password Authentication

Mr.RaghavendracharS   Soumya Dattatreya Hegde   Varsha Purushotham

VennalaKN

Vidyashree S

Department of Computer Science and Engineering  
Visvesvaraya Technological University  
K. S. Institute of Technology, Bangalore, India

**Abstract** - Secret identification numbers are widely used for user authentication and security. Authentication of password using PINs requires users to input the PIN physically, which could be vulnerable to password knowing via shoulder surfing or thermal tracking. Authentication of PIN with hands-off gaze based (by closing the eye) PIN entry techniques, on the other hand, there is no physical footprints behind and therefore offer a more secure password entry option, Gaze -based authentication refers to finding the eye location across sequential image frames, and tracking over 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.

**Keywords** - Recommender system; Collaborative filtering recommendation algorithm; Hierarchical Clustering; Principle Component Analysis; Big Data; Eye tracking; Security.

## 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 Open Cv 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 SURVEY

The paper [1] describes a dynamic gaze gesture-based authentication system to counter shoulder surfing attacks. We also explored two authentication interfaces. In this work, we focus on preventing shoulder surfing attacks on a knowledge-based authentication method, i.e., using passwords specifically in public and semi-private spaces.

The paper [2] presents a method that exploits gaze data to implement a soft biometric technique. Specifically, the user's gaze behaviour is inspected during the unconstrained observation of different kinds of static images. The obtained results, achieved using a machine learning approach. In this paper [3] a simple PIN-like approach to Authentication for using sequence of gaze all observer when presented with a previously seen image on a personal computer screen is proposed. This paper will first provide some background on aspects of the human visual system associated with gaze, and will then describe a general approach to make use of gaze pattern for construction of PIN.

In this paper [4], a system is developed for secure device login that augments face recognition with gaze tracking. SAFE combines face recognition for identification with gaze tracking for the input of a secret. During login, while a face recognizer continuously checks the identity of the user, a number of icons are displayed on the screen; as the icons move in incongruent line patterns, the user follows her/his secret icon with her eyes. By adjusting the number of icons and repetitions, one can control the security of the system.

The paper [5] proposes Eye Dent system which presents an on-screen keyboard (or keypad) to the user, and allows the user to authenticate by looking at the symbols in his/her password in order. The paper [6] presented a study of a potential threat to the Pass Points click-based graphical password scheme, where attackers could use covert eye tracking as a basis for guessing passwords. Gathering actual password click-points from a small sample of users would likely empower more effective

guessing, even though it would take more effort and could not be so easily automated.

In this paper [7], a real-time standalone eye tracking system using a National Instruments Smart Camera is presented with new algorithms. Set of devices and associated programs are integrated for identifying the eye positions and eye movement, and comparing the results to the same eye across images stored sequentially over time.

The paper [8] presents an eye tracking study of Image Pass, a recognition-based graphical authentication mechanism. The mechanism studied in this paper is Image Pass which uses single-object images to build a graphical password with the help of eye tracking.

### III. CONCLUSION

In this paper, we discussed possible way of password authentication by using real time eye tracking. We make use of Smart camera for eye tracking system and it has been incorporated into a new application for gaze based PIN identification. It increases the security of identity authentication mechanism. It has been tested with the nine digit keypad and it can be extended to character and digit combination of password entry. When the entered password equals with the password stored in the memory then the locks gets open. If we enter wrong password then the alarm is switched on. Currently the PIN identification is accomplished after real-time eye tracking and eye center computations and recording are completed. Various measurements were reviewed for the purpose of achieving facial recognition and eye recognition and then distinguish the state of the eye. It can be extended to other applications where camera is used and other mobile applications.

### 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 ; Cynthia Kuo ; Tihomir Lolic ; Ivan Martinovic ; Dawn 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 "Gaze-based 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