iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60664

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Eye Based Secure Authentication System

Nagaraj Shet[1], Amrutha M[2], Prathiksha DM Gowda[3], Vidyashree HR[4]
[1]*Assistant Professor, Dept of CSE Impact College of Engineering and Applied Sciences, Bangalore, Affiliated to VTU*
[2, 3, 4]*Students of Dept of ICEAS, Bangalore, Affiliated to VTU*

Abstract: ***Personal identification numbers are commonly utilized for user verification and enhanced security. When users authenticate passwords through PINs, they must be obligatory to physically input the PIN, making them susceptible to password cracking techniques like shoulder surfing or thermal tracking. In contrast, utilizing hands-off gaze-based PIN entry methods eliminates any physical traces, providing a significantly more secure option for password entry. Gaze-based authentication involves determining the eye location across consecutive image frames and continuously tracking the precise eye center.***
Keywords: PIN authentication, Hands-off authentication, Gaze-based authentication, Eye tracking, Password security

I. INTRODUCTION

One critical aspect of ensuring security for general terminal authentication systems is prioritizing ease, speed, and robust security. With individuals encountering authentication processes daily, relying on traditional knowledge-based methods like passwords poses significant risks due to potential malicious oversight. Threat actors can exploit techniques like shoulder-surfing, where they observe users inputting passwords for unauthorized access, leading to security vulnerabilities stemming from inadequate system-user interactions. Researchers have suggested the use of eye tracking systems to combat this issue. This system provide a secure method for users to enter passwords by choosing the correct symbols in a specified order, effectively preventing shoulder-surfing attempts. In many scenarios, the usage of Personal Identification Numbers (PINs) serves as a common method for user authentication, whether at cash machines (ATMs), electronic authorizations, or device lock/unlock functions. However, verifying these PINs poses challenges for financial and gateway systems, given the rising instances of ATM fraud, which surged by 26% in 2016 according to European ATM Security data. Requiring users to enter their codes in public exposes their PINs and passwords to risks like shoulder-to-shoulder attacks and hot tracking techniques. Eye tracking involves monitoring eye movements across video frames, particularly focusing on head-related eye movements and eye spaces. This technology finds applications in diverse fields like psychological research and visual design. By integrating eye blinking inputs into PIN verification processes, physical traits are negated, enhancing the protection of password inputs significantly. The utilization eye blink verification techniques is an effective method to combat shoulder surfing, data breaches, and various cyber threats prevalent today.

II. LITERATURE SURVEY

[1] This research focuses on using eye blinks as a way to enter personal identification numbers. Traditional password verification through physical PIN entry is susceptible to password theft through methods like shoulder surfing or thermal tracking. "Utilizing eye blinks for PIN authentication, conversely, offers a password input method that leaves no physical traces, ultimately enhancing security". The process involves detecting eye blinks in sequential image frames to generate the PIN. The process includes detecting eye blinks in consecutive image frames to establish the PIN. The initiative presents a real-time system to effectively combat shoulder surfing and thermal tracking attacks. [2] The widespread utilization of Personal Identification Numbers (PIN) for user security and authentication is common. PIN require users to manually enter them, potentially putting passwords at risk of threats such as Shoulder surfing or Thermal tracking methods. Shoulder surfing involves observing someone's shoulder movements to uncover their password, leading to the compromise of sensitive information. Significant security obstacles are challenging to overcome. By implementing Gaze-based authentication, users can securely enter their PIN without the need for manual password input, thereby enhancing security measures. Gaze-based technical authentication relies on tracking eye location and movement for verification purposes.[3] Personal Identification Numbers are commonly used worldwide to ensure secure communication in the processes of user authentication and verification. Despite being widespread, this particular system is not completely foolproof since it remains vulnerable to potential acts of forgery. As the result of manual input required for PINs, they become susceptible to unauthorized access, making them an easy target for intruders using techniques like shoulder surfing, keyloggers, and fingerprint tapping. This paper initiates novel method for creating distinct PINs, which relies on monitoring the movement of the eye pupil.
Users enter their secure PIN by moving their eyes in distinct directions (Left, Center, Right), which is then internally converted into various combinations of numbers from 0 to 9.

[4] Authentication systems utilizing the eye for code entry can be classified in two primary categories: gaze-based and gesture-based. Gaze-based systems necessitate accurate tracking of the user's eye movements, while gesture-based systems concentrate on identifying eye gestures without pinpoint the user's precise focal point. Despite the benefits of gesture-based methods over gaze-based approaches, they encounter difficulties in efficiently recalling multiple gestures the significant memory load involved. To address this challenge, a novel authentication system called (EGBP) has been presented in this study involving eye gesture blink Password. [5] Identification numbers are commonly utilized to verify the identities of individuals and bolster security measures. Password verification using Personal Identification Numbers (PINs) mandates users to physically input the PIN, opening the potential for unauthorized access via tactics such as shoulder surfing or monitoring heat signatures. In contrast, PIN verification using glance-based entry methods leaves no physical traces behind, providing a more secure option for password entry. This study presents a real-time application for visual input of PIN code visual detection of the human eye and verification of the PIN code using a smart camera.

III. OBJECTIVES

The primary concept behind the suggested arrangement involves creating a PIN generation eye based system blinks which relies on computerized vision technology. The identification process involves various techniques such as facial and eye recognition, eye blink detection, and the detection of rectangular. Initially, images from a USB web camera are obtained and analyzed for facial and ocular features of haar cascade classifier. Subsequently, the system utilizes the Histogram of Oriented Gradients (HOG) algorithm to ascertain whether eye is open or closed through eye blink detection. This detection isolates the specific eye region and pinpoints potential circles within the area to accurately locate the eye pupil. Our system incorporates a three-tier authentication approach to enhance user account security, involving facial recognition via LBPH, eye blink-based password generation, and OTP verification.

IV. DESIGN AND IMPLEMENTATION

A. *Implementation*

We hereby confirm that password authentication by flashing method is best technique to prevent current generation shoulder cylinder, thermal attack or other attacks. The advantages provided by the technology outweigh any potential risks it may pose to the users. The process is secure as absence of obligation for users to input their PIN into the machine, and this is simple to swipe the digits and withdraw funds.

1) First run the code.
2) Three windows appear, one is a virtual keyboard, one is for accepting input from the user, and other is used to display the numbers the user has dialed.
3) In the frame window, the individual is captured in real time and their eyes are detected.
4) The numbers depicted in the table windows are used to answer the PIN code.
5) The virtual keyboard has 10 digits (1,2,3,4,5,6,7,8,9,0), E(Enter) and P(Pop).
6) The pop key opens the last dialed number.
7) At the moment the eye remains open, a red line surrounds the eyes.
8) When the user blinks, the color turns green.
9) When the user blinks, the color changes to a number and then we have to blink for a few seconds.
10) If the password matches after entering the password, he will be identified as a authenticated user, otherwise he will have to try another option. of.

B. *Working*

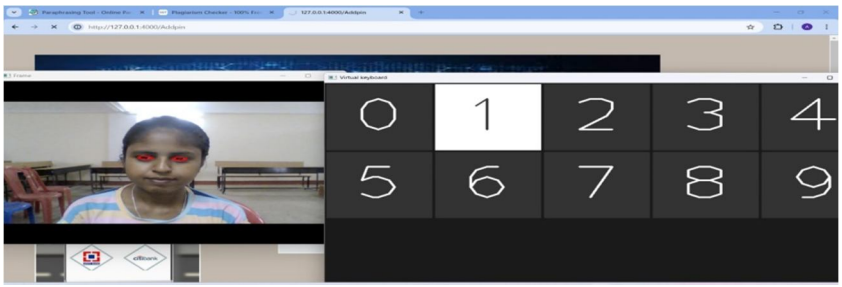


Figure 4.2.1: The personal code of the ATM is "18". The user flashes the number "3", the system takes the input "3", and the user flashes the number 5. The input is "35".

C. Proposed System

The primary concept related to planned system involves creating a method for generating PINs derived from visual observation blinks, relying on computerized vision technology. This process encompasses various techniques including face and eye detection, eye blink identification, detection of rectangular and circular pupil edges, and eye movement tracking. Initially, the system receives images from a USB web camera, proceeds to identify faces and eyes using the haar Cascade classifier, and then determines if an eye is open or closed by leveraging the eye blink detection method with the assistance of the Histogram of Oriented Gradients (HOG) algorithm. Subsequently, the system focuses on the eye region of interest, crops it, and accurately identifies the eye pupil by detecting all potential circles in that specific area. In our proposed system we are combining the three level authentication to secure user accounts, The first level is face recognition using LBPH, Eye blink based password generation and third is OTP verification.

V. DATA FLOW DIAGRAM

A. LBPH Face Reorganization

The algorithm for histogram computation was introduced in 2006 to extract local binary patterns by utilizing the local binary operator. This method is extensively utilized in facial recognition applications due to its straightforward computation and high resolution. The LBPH algorithm is part of Open CV.

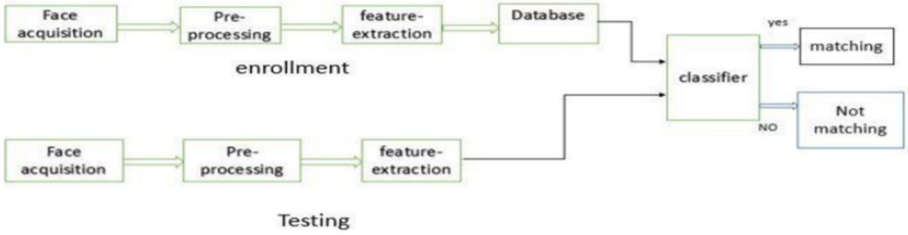


Figure: Data Flow Diagram

VI. METHODOLOGY

Haar Cascade presents a machine algorithm utilizing ML for detection objects in images or videos, developed by Paul Viola and Michael Jones in their paper "Fast Detection of Objects through an Enhanced Sequence of Basic Features". This method uses a cascade function trained on a different types of positive and negative images to recognize objects in new images. The process involves four key stages: selecting Haar features, generating integral images, Adaboost training, and utilizing a Cascading Classifier. The process involves four key stages: selecting Haar features, generating integral images, Adaboost training, and utilizing a Cascading Classifier. Primarily recognized for its capability to recognize faces and body parts, the technology is utilized to distinguish various kinds of objects. In face recognition, the process entails gathering numerous positive and negative facial images to provide training the algorithm and extract relevant features.

VII. RESULTS

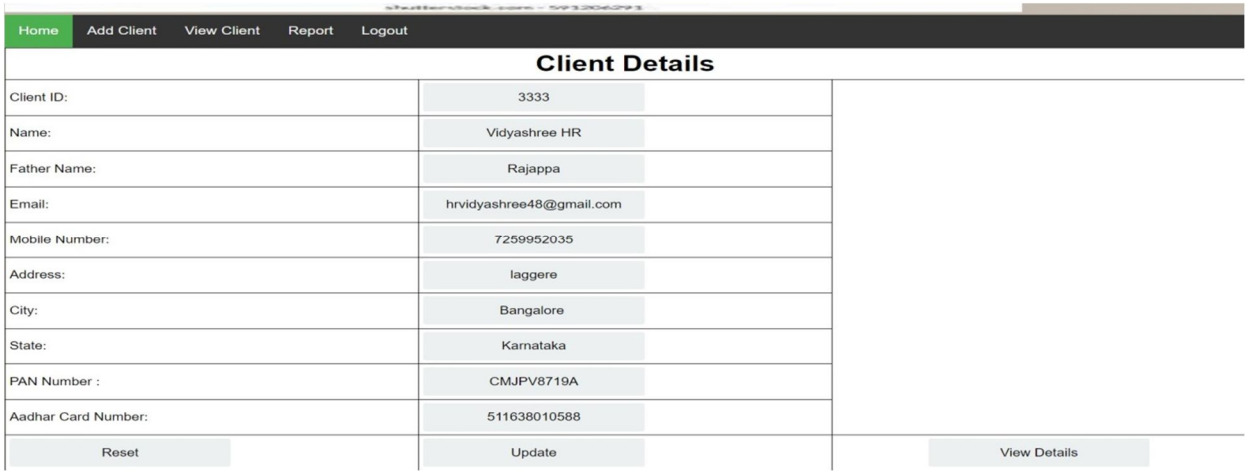


Figure: Client Details

Client ID	Name	Father Name	Email	Mobile Number	Address	City	State	PAN Number	Aadhar Number
1212	Amrutha	Manjunatha AV	mamrutha647@gmail.com	8095012844	byatarayanapura	Bangalore	Karnataka	GM12462	567812549632
3333	Vidyashree HR	Rajappa	hrvidyashree48@gmail.com	7259952035	laggere	Bangalore	Karnataka	CMJPV8719A	511638010588

Figure: Final result

VIII. CONCLUSION

A back camera-based system for tracking eye moments is integrated into a new eye-based PIN recognition application. The system's functionality has been successfully trialed using a nine-digit keyboard and can be extended to allow a combination of characters and numbers for password entry. The accuracy of the system is influenced by the blink rate of numbers. Moreover, it is essential to calibrate the screen size to ensure group accuracy screen and keyboard. The stability of the user's gaze affects the accuracy of detected pins and must be taken into account. After completing real-time eye blinking and recording the blink ratio, the PIN is currently identified.

IX. ACKNOWLEDGMENT

We extend our heartfelt gratitude to the individuals and institutions whose unwavering support and guidance have been instrumental in the successful completion of our assignment.

We are honoured to be linked with ICEAS, an institution that was a pillar of support throughout our journey.

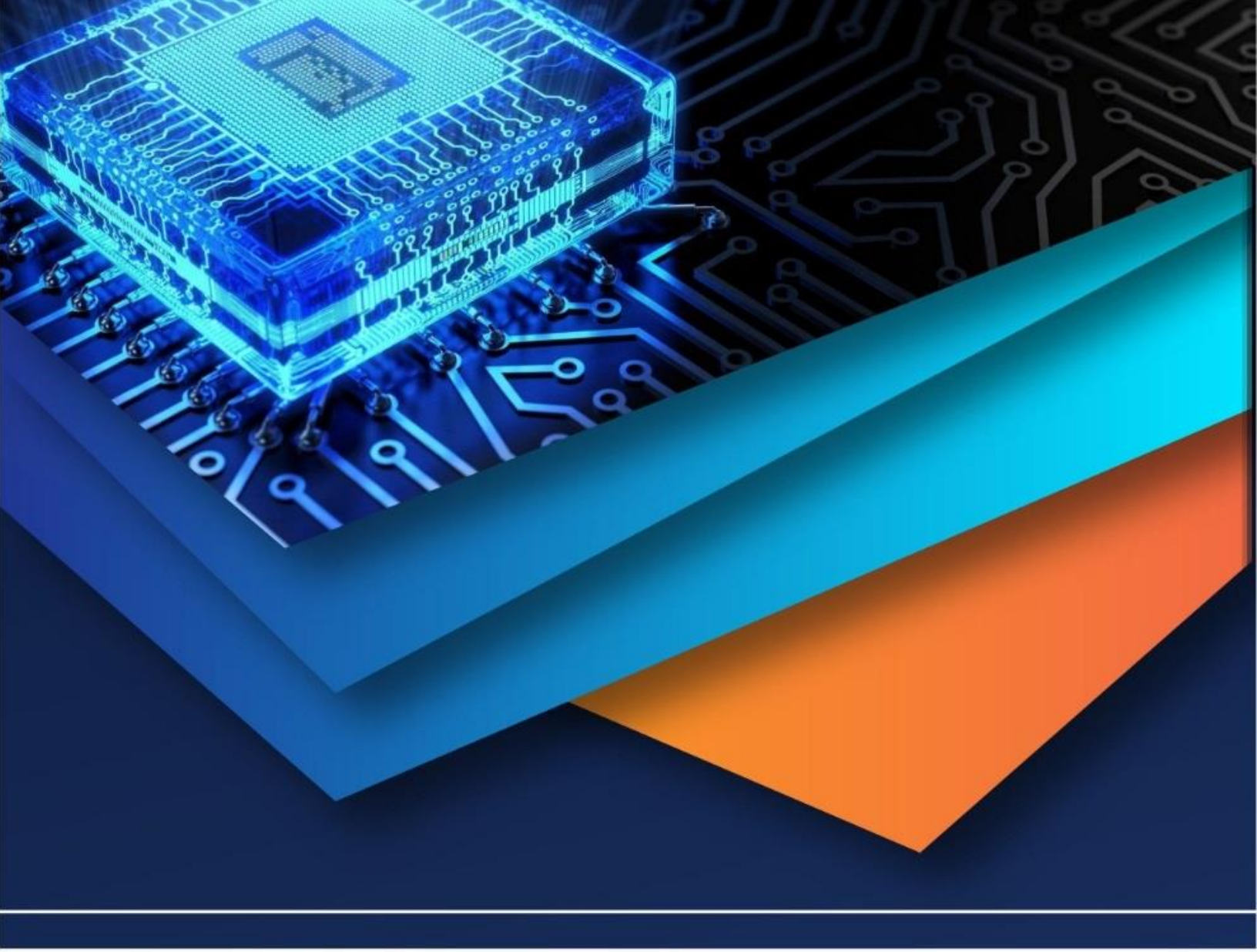
Special thanks to Mr.Nagaraj Shet, Assistant Professor in the Dept of CS&E, for his invaluable guidance and meticulous review of our documents. His dedication and attention to detail have significantly contributed to our project's success.

We extend our sincere gratitude to Dr. Dhananjaya V, Professor and HOD of Computer Science and Engineering, for his invaluable inspiration and guidance, which have steered our efforts in the correct path.

Our sincere gratitude goes to Dr. Jalumedi Babu, the Management for their continuous support and encouragement. We would like to acknowledge the faculty members and supporting staff at ICEAS for their steadfast assistance throughout the project. Lastly, we are grateful to our parents and friends for their unwavering backing and encouragement throughout the duration of our project.

REFERENCES

[1] Asha Rani K P, Asha K N, Nidhi B Channappagoudar, Manonandhan.S, "Realtime Eye Tracking for PA" in IJERT Vol 09 issue 10 October 2020.
[2] Pavitra.S.R,Pushpalatha.S "ET using Gaze Pin Entry for Password Authentication" in IJERT Vol 9 issue 6July 2020.
[3] Indrajith Das, Ria Das, Shalini Singh, Amogh Banerjee, Md.Golam Mohiuddin, Avirup Chowdhury "Design and Implementation of Eye pupil Movement based PIN Authentication System" IEEE Xplore VLSI Device circuit and system July2020.
[4] Hananeh Salehifar, Peyman Bayat "Eye Gesture Blink Password: a new authentication system with high memorable and maximum password length" in Springer June 2019.
[5] Dr.A.Syed Mustafa, Syed Zaid, Tasmiya Banu, Aparna Nair "Automated eye Tracking Mechanism for Password Authentication" in International Research Journal on advanced Science Hub 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY