RESEARCH ARTICLE **SPECIAL ISSUE**

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
Vol. 05 , Issue 05S May
www.rspsciencehub.com

Check for updates

http://dx.doi.org/10.47392/irjash.2023.S001

International Conference on intelligent COMPUting TEchnologies and Research (i-COMPUTER) 2023

Real time eye based Password Authentication by Eye Blinking System

Buddesab[1], Nanda Ashwin[2], Shruthi M [3], Rekha P [4], Pavan Mulgund[5]

[1]Associate Professor, Department of AIML, Cambridge Institute of Technology, Bangalore-560036, Karnataka, India
[2]Professor, Department of ISE, East Point college of Engineering and Technology, Bangalore-560049, Karnataka, India
[3]Assistant Professor, Department of CSE, The Oxford College Engineering, Bangalore-560068, Karnataka, India
[4]Assistant Professor, Department of ISE, MVJ Engineering college, Bangalore-560067, Karnataka, India
[5]Assistant Professor, Department of ISE, East Point college of Engineering and Technology, Bangalore-560049, Karnataka, India

Email: tonnur21@gmail.com

Article History

Received: 15 February 2023
Accepted: 13 March 2023

Keywords:

Corona Virus;
Chest XRay;
Convolutional neural networks;
Detection

Abstract

The focus of this work is on PIN entering utilising the blinking approach, for user authentication and security, personal identification numbers are employed. PIN-based password verification users must input a physical PIN that can be cracked or hacked using shoulder surfing PIN entry process using eye blinks entering does not provide or easily leave any footprints behind, making it a more secure password entry option. Locating the blinks of an eye over creating picture frames in a consecutive order the Personal identification number is referred to as eye blinks-based authentication. This research shows how to resist shoulder surfing and thermal tracking attacks in real time. Today's authentication technologies, such as passwords, fingerprint scanners, and PIN entry, are all based on one-time, static authentication mechanisms that are vulnerable to assaults. The Real-time eye monitoring and password authentication methods are being used has a greater chance of being reliable, In this case, the system for Eye Detection and Tracking must be secure and limited.

1. Introduction

Online system has now become an integral part of our daily lives, with all services moving online. We have grown regular repetition to various risky tasks, like purchasing with credit cards, email check/compose, internet banking, and so on, in addition to reading the news, hunting for information, and other duties that are not dangerous. We are putting ourselves at risk while appreciating its benefits (Mock et al.) (Bhavyashree, Thriveni, and Venugopal).

For user authentication and security, personal identification numbers are commonly utilised. PIN-based pent authentication users are required to physically enter the PIN, exposing it to sword cracking through shoulder surfing or thermal monitoring. Personal identification number authentication using personal identity number physical entry process based on sight, on the other hand, we will not physical traces left at any places, and thus provide a stronger password entering option. Gaze type authentication is a process of locating the eye across many visual tracking the eye centre over time. The project uses a smart camera to demonstrate a real-time eye blinking technology to enter the password, as well as eye recognition and tracking for PIN identification (Mehrube and Nguyen).

Authentication methods are frequently presented to people and must use conventional means of authentication knowledge-based approaches such as

entering passwords, hence one of the safety measures requirements it is recommended that general terminal authentication methods be implemented simple, quick, and secure. These methods however, are insecure because hostile observe can observe them who utilise observation like shoulder-surfing (observing a user while password on the keyboard) to acquire user authentication data. There are also issues with security as a result of bad relationships between users and systems. As per the result obtained, people who are working for it has devised a to defend yourself, use a three-layered security system. PIN numbers, in which the password is entered by blinking their eyes at to relevant symbols in write order, making them immune to shoulder surfing (Das et al.) (Buddesab, Thriveni, and Venugopal).

2. Literature View

Eye Pass Shapes enhances and advances two authentication systems, Pass Sha**pe**s and Eye PIN, by merging them, as Alexander, Martin, and Heinrich (2009) propose (e-ISSN: 2395-0056) "Eye-Pass Shapes Method." Users in Pass Shape must paint shapes in a specific order; this method improves security but not memorability when compared to password entry. Eye based PIN security is given precedence above usability (Mustafa and Syed).

CGP improvements, presented by Alain, Sonia, and Robert (2010), can be thought of a method of defending against graphical passwords such attacks using Instead of mouse clicks, eye-gaze pass-word input is used, but it necessitates particular ways for enhancing gaze accuracy. Two breakthroughs were presented in this work: a nearest-neighbor gaze-point aggregation method and one-point calibration prior to entering the pass-word. They came to the conclusion that the adjustments significantly improved the precision of users' sight and the efficiency of the system.

Eye Pupil Movement Based PIN Authentication System Design and Implementation was developed in 2020 by Indrajit Das, Ria Das (ISSN No. 0976-5697) etc. The detection of whether an eye is open or closed is successful 92.51% of the time, while the accuracy of the eye detection method is 98%. Finally, the work's contribution is detailed, and a comparison of the created system with classic gaze, touch, eye movement, and gaze use of CAPTCHA and graphical image-based authentication methods is being pursued (Mehrubeoglu and Nguyen).

"Realtime Eye Tracking for Password Authentication" which was developed in 2020 by Asha Rani K P, Asha K N (ISSN: 2278-0181) (Mehrube and Nguyen). The excellent accuracy of the results stated in the preceding section, the system's reliability has been demonstrated. The system functions exceptionally well in severe lighting settings (i.e., when lights turned off, leaving only the computer's screen as a source of light, and a bulb which used to provide vedio), according to the trials. In these circumstances, the accuracy percentages were similar to those obtained under normal lighting.

Password Authentication via Eye Tracking Using Gaze Pin Entry Mrs. Pavitra S R and Mrs. Pushpalatha S created Eye Tracking with Gaze Pin Entry for Password Authentication in the year 2020 (ISSN: 2278-0181). Because of the ease of access to processing and equipment assets, as well as the expanding demand for human PC collaboration techniques, eye stare estimation is an interdisciplinary topic of new work that has piqued the interest of academic, modern, and general client networks in recent decades (Rahman et al.) (Pushya).

3. Proposed work

The graphic below depicts the exact operation of the proposed system's password authentication model. Recognizing the face is the first step in the execution. The only way to detect blinking and analyses blink duration is to look at the correlation scores collected from the user's eye's online template during the previous stage's tracking. The likeness of the user's eye to the open eye template reduces when the user's eye closes throughout the blinking process. When the blinking ceases, the user's perspective completely opens over, it regains its likeness to the template. The correlation values given by the template matching technique correspond exactly to the decrease and rise in similarity as shown in **Figure 1**.

It initially started with registration phase in which registration of individual should register. While registration person should choose a id number and create own password. Then it is passed to training phase where it is completely trained by HAAR cascade algorithm. Then after training phase and system will identify the user id and password by

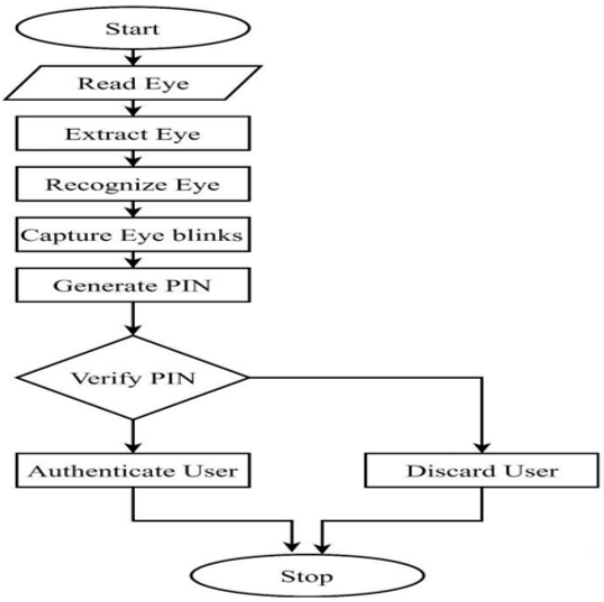

FIGURE 1. Proposed Work flow chart diagram

LBPH(local pattern histogram algorithm). Then individual should blink eyes and try to enter the password and in the later state it will check the database if the database matches then there will transaction process. Eye tracking, also known as eye gaze tracking, is a method of recognizing the position of the eyes using video record outlines. The eye's development in relation to the head may have a few effects as well. This technique can help handicapped people talk by using deliberate motions such as facial, eye, and nose development. Users with minor disabilities may also benefit from PC access to commonplace activities such as playing games and surfing the internet. Eye tracking technology is used, which uses a simple web camera to watch a person's eye movement and changes the cursor as needed.

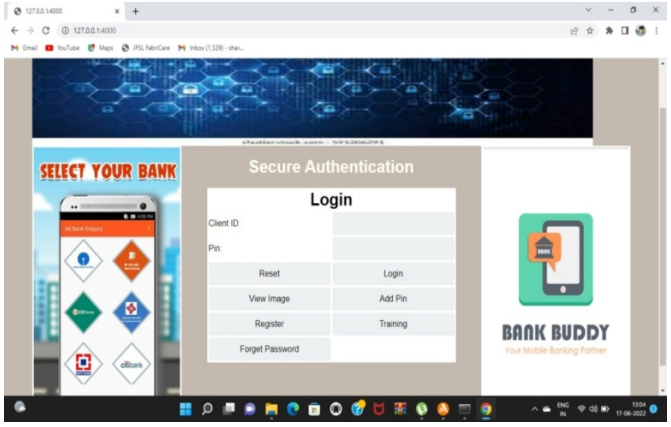

FIGURE 2. Login page

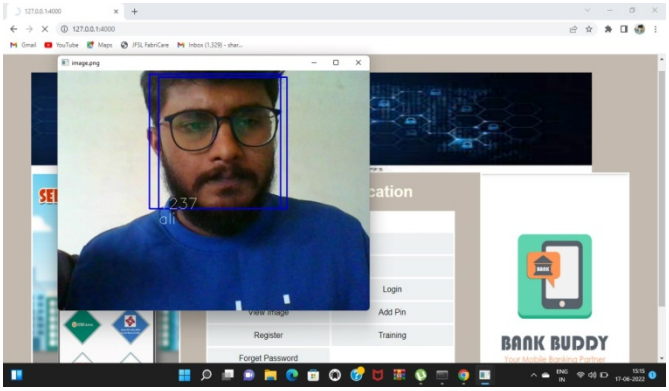

FIGURE 3. System identifying user id and name

4. Implementation environment

4.1. Machine Learning

Machine learning is a branch of computer science that studies and develops methods for 'learning,' or using data to improve performance on a set of tasks. It is regarded as a part of artificial intelligence. Machine learning is significant because it allows businesses to see trends in customer behavior and company processes, as well as aid of developing best goods. Machine learning is the best tool for the success of many companies, like Uber, Google and Facebook. For many firms, machine learning is the key to success (Masini et al.) (Burés, Jordi, and Larrosa).

4.2. HAAR cascade algorithm

It's a real-time Object Detection Algorithm that detects faces in images and movies. Viola and Jones proposed edge or line detection features in their 2001 study "Rapid Object Detection using a Boosted Cascade of Simple Features" (Viola, Paul, and Jones). A big number of positive photos with faces and a large number of negative shots with no faces are provided to the algorithm to train on. There are four stages to the HAAR cascade algorithm (Phuc et al.):

1. HAAR feature selection.
2. Creating integral image.
3. Adaboost training.
4. Cascading classifiers.

The Figure 4 shows creating integral image where eye are tested horizontally, vertically, sideways etc. And cascading classifier identifies positive and negative images and differentiates both and could be represented in Figure 5.

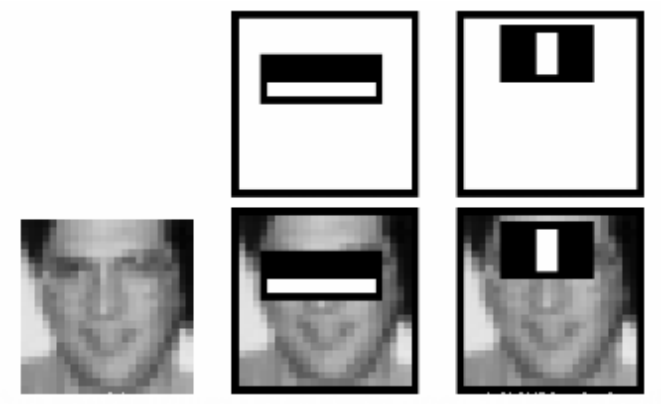

FIGURE 4. Creating integral image

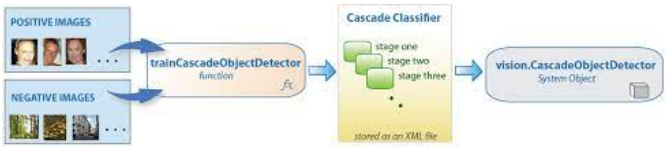

FIGURE 5. Cascading classifiers representation

4.3. LBPH(Local Pattern Histogram Algorithm

The most frequent method (Chinimilli et al.) (K. C. Paul and Aslan), however, is to extract LBPH code from each 3*3 window in the image. We need the central pixel value and the neighbour pixel value to calculate the lbp code. Consider the following example: -82 is the value of the central pixel. Pixel values of neighbours: 137,135,115... and is given in Figure 6.

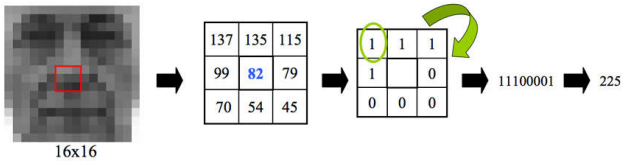

FIGURE 6. LBPH working process

4.4. AdaBoost Algorithm

In 1997, Freund and Schapire have proposed boosting as an ensemble modeling technique, and until now it has been one of the popular methods to solve binary classification issues (Ying). It has turned a weak learner to strong learner and these types of methods have helped to boost prediction power. These boosting algorithm which are present works based on initially builds a model which are required for the dataset and then to correct the faults which are developed at initial stage.

This technique is performed again and again until it has been reduced to a minimum and the dataset has been correctly forecasted. AdaBoost, which is known as Adaptive booster, is a type of Machine Learning method that is used as part of an Ensemble Method. Decision trees which contain only one leaf, or Decision trees which contain only one split, these are one of the popular methods which can be called as algorithm which are used in AdaBoost. Other names of these trees are called Decision Stumps.

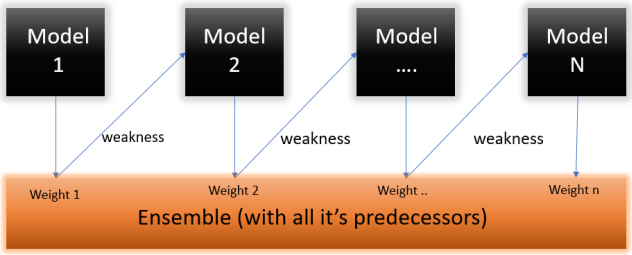

FIGURE 7. AdaBoostAlgorithm

We are completed the job using the above algorithm. The 1-9 key pads were produced using opens. The automatic movement of the cursor is also visible in this keypad. The registered user can enter the password by blinking his eyelids. If a person's password matches the database, he can proceed with the transaction or any other procedure. Keypad and password enter is explained in Figure 8.

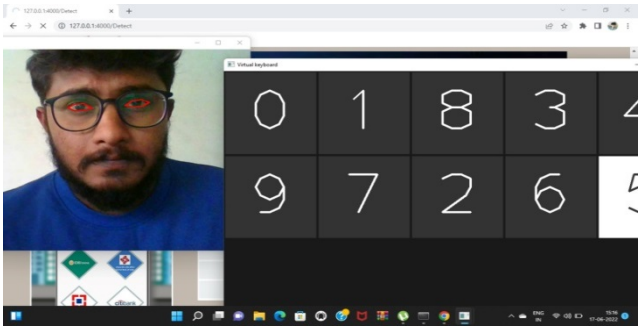

FIGURE 8. Password entry by blinking eye

5. Results

The vast amount of information which was collected to perform test the machine's accuracy, and every operation performed were executed well. The Proposed Work flow full implementation is depicted in Figure 1. Without manually entering the PIN, the password can be verified. Shoulder-surfing, thermal hacking and other threats to the user are avoided

TABLE 1. Performance parameter of gaze based detection and eye blinking system

	Performed in gaze based detection	Performance using eye blinking system
Efficiency	Low efficiency	High efficient
Availability	Person facing problem is eye have some issues	Most of all could easily handle it
Duration	It takes few minutes to handle	It could handle in seconds
Expenses	More Expensive	Cost Efficient
Execution	It is hard to execute	Very simple to execute

with this strategy. This is the most secure method of PIN authentication.

The difference between them easily tells us that the eye blinking method of password authentication is clearly dominant than the other method present. This model was tested on a large number of cases with the conditions ”PASSWORD MATCH” and ”PASSWORD NOT MATCH” and others, and all of the cases were more than 90% efficient. It is one of the different technologies which has not yet used until present days and it could replace the physical entry of PIN which used in present technology, which can lead to risks such as shoulder-surfing, thermal hacking, and so on. The objective of this system is that there is nothing required implementing different product to design, therefore even the system's design can be an empty background.

6. Conclusion

The main aim of our Paper provide three layers of security in which the algorithm which detect the face of individual face and produce user identification number and also the name have been generated. In second layer person should enter the password by blinking his eyes as to avoid from shoulder surface or thermal surface attack. Then at last our project will generate a automatic one time password to registered number and by passing all of these our project has provide one the best and secure protection have been provided. This strategy overcomes the main disadvantage of forgetting your passwords and allowing them to be leaked, and it is the safest alternative for the same. The application of this technology will benefit every sector of the business world. By developing some further modifications and conducting more study at a higher level, this technology can be employed for high-end security systems.

Authors' Note

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the pa-per was free of plagiarism.

References

Bhavyashree, S P, J Thriveni, and K R Venugopal. “Integration of Wireless Sensor Network and Cloud Computing Using Trust and Reputation Technique”. *Proceedings of International Conference*. Springer, 2018.

Buddesab, Thriveni, J Thriveni, and K R Venugopal. “Trust model genetic node recovery based on cloud theory for underwater acoustic sensor network”. *International Journal of Electrical and Computer Engineering* 9 (2019): 3759–3771. 10.11591/ijece.v9i5.pp3759-3771.

Burés, Jordi, and Igor Larrosa. “Organic reaction mechanism classification using machine learning”. *Nature* 613 (2023): 689–695. 10 . 48420 / 16965292.

Chinimilli, Bharath Tej, et al. “Face Recognition based Attendance System using Haar Cascade and Local Binary Pattern Histogram Algorithm”. *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)* (2020). 10.1109/ICOEI48184.2020.9143046.

Das, Indrajit, et al. “Design and Implementation of Eye Pupil Movement Based PIN Authentication System”. *2020 IEEE VLSI DEVICE CIRCUIT AND SYSTEM (VLSI DCS)* (2020). 10 . 1109 / VLSIDCS47293.2020.9179933.

Masini, et al. “Machine learning advances for time series forecasting”. *Journal of Economic Surveys* 37.1 (2023): 76–111. 10.1111/joes.12429.

Mehrube, Mehrubeoglu and Vuong Nguyen. “Real-time eye tracking for password authentication”.

2018 IEEE International Conference on Consumer Electronics (ICCE) (2018). 10.1109/ICCE.2018.8326302.

Mehrubeoglu, Mehrube and Vuong Nguyen. "Real-time eye tracking for password authentication". *2018 IEEE International Conference on Consumer Electronics (ICCE)* (2018). 10.1109/ICCE.2018.8326302.

Mock, Kenrick, et al. "Real-time continuous iris recognition for authentication using an eye tracker". *Proceedings of the 2012 ACM conference on Computer and communications security* (2012). 10.1145/2382196.2382307.

Paul, Kamal Chandra and Semih Aslan. "An Improved Real-Time Face Recognition System at Low Resolution Based on Local Binary Pattern Histogram Algorithm and CLAHE". *Optics and Photonics Journal* 11.04 (2021): 63–78. 10.48550/arXiv.2104.07234.

Phuc, Le Tran Huu, et al. "Applying the Haar-cascade Algorithm for Detecting Safety Equipment in Safety Management Systems for Multiple Working Environments". *Electronics* 8.10 (2019): 1079–1079. 10.3390/electronics8101079.

Pushya, D. "FDMCA: A Novel Authentication Technique using Face Detection and Gaze-based Morse Code Entry". *2021 IEEE Mysore Sub Section International Conference (MysuruCon)* (2021). 10 . 1109 / MysuruCon52639 . 2021 . 9641520.

Rahman, et al. "REAL TIME EYE TRACKING FOR PASSWORD AUTHENTICATION". *International Journal of Advanced Research in Computer Science* 11.3 (2020): 50–54. 10 . 26483 / ijarcs.v11i3.6599.

Viola, Paul, and M Jones. "Rapid object detection using a boosted cascade of simple features". *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001* 1 (2001). 10 . 1109 / CVPR.2001.990517.

Ying, Cao. "Advance and prospects of AdaBoost algorithm". *Acta Automatica Sinica* 39 (2013): 745–758. 10.1016/S1874-1029(13)60052.

Embargo period: The article has no embargo period.

To cite this Article: Buddesab, , Nanda Ashwin, Shruthi M , Rekha P , and Pavan Mulgund. "**Real time eye based Password Authentication by Eye Blinking System**." International Research Journal on Advanced Science Hub 05 .05S May (2023): 1–6. http://dx.doi.org/10.47392/irjash.2023.S001