



Eye blink Password Based Secure Authentication

Malar K¹, Nayan Kumar S², Ravi N³, Rohith Kumar G M⁴, Yuva Kishor TM⁵

¹Assistant Professor, Department of Computer Science and Systems Engineering, Sri Sairam College of Engineering, Bangalore – 560126

^{2, 3, 4, 5}Final Year, Department of Computer Science and Engineering, Sri Sairam College of Engineering, Bangalore - 560126

ABSTRACT

An eye blink password based secure authentication system utilizes the unique biometric patterns found in the human eye, particularly the iris or retina, to verify an individual's identity. This technology capitalizes on the distinct and stable nature of eye biometrics, making it highly secure and reliable. The system involves capturing high-resolution images of the iris or retina, extracting unique features, and matching them against a stored database for authentication. Due to its accuracy, it is ideal for high-security applications where traditional methods like passwords may fall short. Integrated with encryption and liveness detection, eye-based authentication prevents unauthorized access and is resilient against spoofing attempts, offering a robust, non-invasive solution for secure identity verification. 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.

1 Introduction

The eye blink password based secure authentication systems represent the next generation in biometric security, making use of the unique properties of the human eye and, specifically, the iris and retina, to give a very secure and reliable method for authenticating individuals. This form of authentication is completely different from those that most people are accustomed to with regard to passwords or ID cards. Eye-based systems have the form of recognition, which is highly difficult to forge or reproduce because, just like with fingerprints, no two persons have similar iris and retina patterns that remain unchanged over time. It is the process of capturing a high-resolution image of an eye and further processing it to determine unique features. The unique features are matched against a secure database; entry is allowed in case there is a match. Such a system with accuracy and efficiency becomes significant for sectors that involve a high level of security such as banking, healthcare services, and government facilities. Given such advances in encryption and liveness detection, eye-based authentication systems offer not only non-invasive means for authentication of identity but also excellent protection against frauds, spoofing, and unauthorized access, which make the biometrics of eyes a promising candidate to change the future of secure authentication. This system avails the secured input for passwords when a user clicks the appropriate symbol in proper sequence



which keeps away the shoulder surfing. Very many times, use of PIN is common authentication used on the side of users. Whether through ATM or electronic authorization as well as one's devices unlock and lock function but their validation challenges to financial and access systems due to the increasingly frequent ATM fraud cases, that increased by 26% in 2016 by European ATM Security statistics. Asking a user to insert his/her codes in the public increases the chances that the person's PIN and password get compromised by tactics such as shoulder-to shoulder attacks and even hot tracking technique.

2 Recent Works

All the previous pupil tracking-based authentication systems use the commercial eye tracker in order to obtain an accurate user's perspective which involves a calibration step. The difference between the previous systems in various designs is that the user is supposed to enter the password, therefore resulting in a difference in the login time and the error rate. In such systems, the way the user's password is found. Not taken into account by the commercial eye tracker as it detects the viewpoint of the user. Even in gesture-based systems, the track of the viewpoint of the user that is detected forms the gesture. The goal of this work is to present the novel eye movement analysis-based authentication system known as EGBP. The EGBP was the first authentication system which is presented without the use of a commercial eye tracker and eliminating the calibration step. This System, the first time plan, where the user password is able to be predicted sequentially using its sequence without definitely set of viewpoint. In such plan, where it makes a matter of difference which site does the user gazes but it is significant whether the angle between them the sites, extracted as being fixations. It doesn't use an eye tracker. The system is of low cost. The system doesn't require a calibration step. It uses eye fixations and angle between fixations to decode password. Thus it processes faster and makes use of inexpensive hardware setup. Here in this method, person produces directional vectors by shifting any one of the sequences of points, which could be treated as a password. As the password is a pattern, so it is more easy to memorize than the numeric code-based methods. Special features of this system help the user to blink as a password. One of the main aims of this project are high numbers of entered different passwords for a fixed length of the code, and that is achievable with the concept of blinking.

3 Proposed Work

The most relevant concept based on a planned system was to develop an approach in creating PINs generated using the observation of blink with computer vision. All this was contained within detection of face and eye; detection of rectangular, circular and even the edges of pupil or eyes' movement. This device is fed by images from a USB web camera, continues to detect faces and eyes using the haar Cascade classifier, and later determines whether an eye is open or closed based on the eye blink detection method with the help of the Histogram of Oriented Gradients (HOG) algorithm. The system then targets the eye region of interest, crops it, and accurately identifies the eye pupil by Detect all the possible circles in that particular region. In our proposed system, we are using three level authentication to secure user accounts. First, it



is face recognition by using LBPH, Eye blink based password generation, and third OTP verification.



Figure 1: Proposed block diagram

2.1 Mathematical Expressions and Symbols

In password-based authentication employed in the eye-blink, mathematical expressions and symbols are of significant importance while modeling tracking, detection, and processing of eye blink. Some of the most essential elements are these: Key Elements and Their Mathematical Expressions

1. Detection of Eye Blink

In the eye-region frames captured by the system, the system further calculates the Eye Aspect Ratio EAR, a metric most used for blink detection:

$$EAR = \frac{||p_2 - p_6|| + ||p_3 - p_5||}{||p_1 - p_4||}$$

Here, $p_1, p_2, \dots, p_6$ are coordinates of some important points near the eye. If the EAR falls below a threshold T_{blink} , it means a blink.

2. Blink Sequence Encoding for Password Generation

Let B_i be the blink sequence with i as the index for each blink. A password can be formed by timing intervals or patterns between blinks:

Password = $f(B_1, B_2, \dots, B_n)$ Blink-based time interval: Let (t_i) denote the time of blink (B_i) , then the time interval between two consecutive blinks is defined as $\Delta t_i = t_{i+1} - t_i$.

3. Blink-based selection pattern

Based encoding A virtual on-screen digital keypad is used. The cursor blinks over each digit. A selection function, (S) maps the blinks to selected numbers

$$S(B_i) = N_j$$

Here, N_j is the digit selected at the blink B_i when the cursor is on j .

4. Authentication Probability Model

Estimate the probability that the legitimate user blinks in a pattern unique to the user



(authentication pass). First, calculate the probability using the patterns specific to the user and the time intervals between Delta blinks:

$$\square_{\text{auth}} = \prod_{i=1}^n (\square_i | \Delta \square_i)$$

5. Error Tolerance and Thresholding

Define an acceptable error threshold (E) to tolerate minor variations in blink patterns due to natural variability:

Accept if $|t_i - t'_i| < E$

Here, t'_i is the observed blink timing, and t_i is the expected timing for a legitimate user

4 Results and Discussion

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

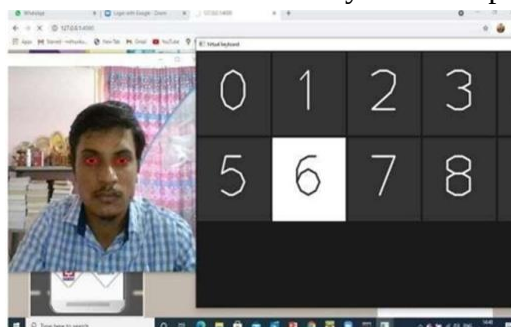


Figure 2: virtual keyboard to add pin through eye blink



5 Conclusion

A 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.

References

1. K. P. Asha Rani; K. N. Asha; Nidhi B. Channappagoudar; S. Manonandhan, Year: 2020, "Real time Eye Tracking for Password Authentication (PA)", in IJERT, Vol: 9, no: 10.
2. S. R. Pavitra; S. Pushpalatha, Year: 2020, "Eye Tracking using Gaze PIN Entry for Password Authentication", in IJERT, Vol: 9, no: 6.
3. Indrajith Das; Ria Das; Shalini Singh; Amogh Banerjee; Md. Golam Mohiuddin; Avirup Chowdhury, Year: 2020, "Design and Implementation of Eye Pupil Movement-based PIN Authentication System", in IEEE Xplore, within the conference on VLSI Device, Circuit, and System, published in July 2020.
4. Hananeh Salehifar; Peyman Bayat, Year: 2019, "Eye Gesture Blink Password: A New Authentication System with High Memorability and Maximum Password Length", in Springer, published in June 2019.
5. A. Syed Mustafa; Syed Zaid; Tasmiya Banu; Aparna Nair explored, Year: 2021, "Automated Eye Tracking Mechanism for Password Authentication", in the International Research Journal on Advanced Science Hub, published in 2021.