International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || PP. 10-15

A Survey on Real-Time Eye Blink for Password Authentication System

Nagashree.S[1], Abhinav Aditya[2], Divya Kumari[3], Alka Suman[4], Akshaya Raj[5]
Department of Information Science and Engineering ,JSS Academy Of Technical Education Banganlore, India

Abstract :*People commonly use real time password authentication techniques, which can be broken or hacked using a high-speed scan or hot track. Pin verification with blinding hand gestures, does not leave visible fingerprints and thus provides a more secure way to enter the password. Blink-based authentication is the process of blinking the eyes with multiple photo frames and creating a PIN. This paper represents a variety of real-time applications that avoid shoulder-to-shoulder and scratch tracking by combining instant-based PIN, face detection, and One-time Password.*

Keywords: *Eye Blink, LPBPH,* ***,*** *HAAR Cascade ,HOG Algorithm, PIN Authentication,*

I. Introduction

The use of personal identification number (PINs) is a familiar way to authenticate a user in many applications, such as cash register (ATMs), electronic authorization, locking and unlocking personal devices. Even though using personal identification numbers, verification is a challenging task for financial and gateway systems.[1] According to European ATM Security, ATM scams increased by 26% in 2016. The fact is that the authorized user enters the code in public makes the PIN and password vulnerable to shoulder-to-shoulder attack and hot tracking.Eye tracking is the mechanism of finding eye space throughout the video frame. Head-related eye movements have an added interest in following the eye.[1] Tracking of eye movement is used in development and research areas such as psychological analysis and visual design. The eye tracking system is a combination of a set of devices and compatible systems for measuring eye movements and associating the results of the same eye on images obtained in chronological order. PIN verification based on eye blinking input method dissolve any physical traits and hence offers a more guided password entry method.[7] Eye blink verification extracts instantaneous eye blinks in all frames of image to produce PIN. Thus the password verification using eye blink approach is the best way to prevent shoulder strokes, heat attacks and any other type of attack in the current generation. This technology has many advantages over any other authentication methods. In this approach the user doesn't have to enter the PIN digits manually, instead they have to eye blink the digits and extract the PIN values. The purpose of this review paper is to understand the current research related to real time password verification techniques. The paper is organised as follows: Section 1 gives a detailed description of password authentication system available in literature. Section 2 describes various research work carried on eye blink password authentication using machine learning and deep learning. Section 3 gives the conclusion.

1. Various Password authentication systems

This section describes various password authentication system that is been used in the society**.**

1.1 Standard Password Authentication

Common password verification involves the user entering his or her user name, followed by a set of code or password that allows him or her to access any internet application. Cyber criminals use programs that test thousands of passwords and gain access to the right one. To reduce this risk, users need to choose secure passwords consisting of both numbers and letters, uppercase and lowercase, special characters such as $,%, or & and words that are not found in the dictionary [3]. It is also important to use at least a length of eight characters.

1.2 Two-Factor Authentication (2FA)

Two-factor authentication, or a variety of multi-factor authentication, constructs on passwords to create a more powerful protection solution. A password functions like "something you know," and having something tangible like a smartphone works like "something you own." In computer security, 2FA follows the same principle. After entering their username and password, users must clear an additional barrier to login: they need to enter a one-time code from a specific mobile device. The code can be sent to their cell phone via text message, or it can be generated using a mobile app. If a criminal guesses a password, it will not be able to proceed without the user's cell phone; conversely, if they steal a mobile device, they cannot log in without a password. 2FA is used in a growing number of banks, emails, and social media websites.

1.3 Token Authentication

Token systems use a virtual device designed for the purpose of providing two-factor authentication. This could be a dongle inserted into the USB port of your device, or perhaps a smart card with a radio frequency identification card or a chip near the location. If only a team member is hired, for example, they should give up their token. These systems are more expensive as they require the purchase of new equipment, but can provide an additional level of security.

1.4 Biometric Authentication

Biometrics depends on the user's physical characteristics for identification. This is a very secure type of authenticity because no two people will have the same physical features. The most common biometric systems use fingerprints, retinal scans or iris, voice recognition, and facial recognition. Since no two users have the same visual features, biometric authentication is much safer. It is the only way to know for sure who is accessing the system. One advantage is the user does not need to remember the password.

1.5 Computer Recognition Authentication

Computer recognition is a password verification method that verifies user authentication by looking at a specific device. These systems install a small software plug-in on the user's device when they first log in successfully. This plug-in contains a cryptographic device tag. When the user next logs in, the marker is checked to make sure you are on the same, trusted device. The advantage of this program is that it is not visible to the user, who simply enters his username and password; verification is done automatically.

1.6 CAPTCHA

The program displays a distorted image of letters and numbers on the user, asking them to type what they see. Computers have a hard time dealing with this distortion, but people are able to say what they are. Adding a CAPTCHA improves network security by creating another barrier to auto-hacking systems. CAPTCHAs do not focus on validating a particular user, as some of the methods listed in this article do. Instead, CAPTCHAs aim to determine if a user is human, preventing computer-driven attempts to access accounts such as violent attacks.

II. Literature Survey On Eye Blink Password Authentication Using Machine Learning And Deep Learning

In this paper [1] PIN is used to authenticate users. Password verification requires that the PIN be entered automatically, which is unsafe for password violations or hacked hot purses or shoulder straps. The blinking process does not leave any physical appearance behind and therefore offers a more secure password entry option. Ensuring eye blinking refers to tracking the blink of an eye on all consecutive image frames and the production of a pin. Results were compiled based on the number of shoulder blades, DAS only, DAS only, and Decoy Stroke defenses had a moderate stroke of approximately 77%, while Disappearing Stroke and Line Snaking defenses were between -40 % and 50% are partial. A large amount of information has been created to achieve system accuracy. This is the safest way to verify a PIN. this test shows that the system works best in extreme light conditions and the accuracy in these cases is 100% and the same as those downloaded with regular lights.

This paper [2] focuses mainly on real-time outputs and focus-based PINs, tracking eye movements and seeing eye position using a smart camera. Real-time eye tracking provides an important way for patients with disabilities, online surveys, surveillance encryption and home security applications. In order to protect and secure (verify) user ID numbers are used abroad thus reducing the chances of attack. For static verification methods, since the password must be entered automatically using PIN's there is a possibility to track the password using shoulder surfing, to avoid this spy password tracking game, using eye-focused PIN insertion techniques. The smart camera is used to detect eye area and Gaze-based PIN Identification thus facilitates data processing .The smart eye tracking system uses Hough circle rotation to detect the circle, blink detection is used to mimic the input key board. To control the position of the mouse, the eyeball position is used. Introduced Many reviews of the professional tennis eye movement skill to measure eye movement with respect to 2 categories namely professionals and beginners. The proposed system namely EEG pattern recognition related to real-time BMI eye movement intended for rapid BMI pattern recognition of the ball movement.

In this paper [3] a PIN based eye reader is created. The user enters a PIN using his or her eye reader movement in a variety of ways, which are drawn internally in sequences of various digits from 0 to 9. This utilizes the HAAR Cascade facial and eye detection section in an integrated way with HOG features integrated with SVM blink blinker. adoption. The accuracy of eye detection, blink vision and eye tracking are 98%, 92.51% and 96.25% respectively. this [3] was presented as well as a comparative study between the proposed method and traditional verification systems such as glare, glare - touch, eye movement CAPTCHA and image-based verification methods. The process begins when the system detects images captured by the USB web camera.and then perform facial and eye detection with the Haar Cascade section which is followed by whether the eye is openor near the way to get a blink with the help of the Histogram of Oriented Gradients (HOG) algorithm. The aim is to find the rectangle and circle of the eye reader through the discovery of the canny edge and the Hough Circle Transform (HCT) system respectively. Internal database built, eye-catching class by Haar Cascade class divisions with 98% accuracy. In some cases, to find out if the eye is open or closed, 144 HOG elements of eye images are extracted. These are used in the SVM separator, which then indicates whether the eye is open or closed. There are 294 eye photographs in the test, which includes 147 open and 147 closed eyes, the accuracy of the open and closed eye is 92.51.

This paper shows a continuous PIN corridor application based on appearance, in addition, eye tracking and tracking to obtain visual PIN evidence using a smart camera. The eye tracker-based entry is an entry control system that allows newly authorized people to reach a limited area. The frame has a PC with openCV and a camera with which to enter the password. When the entered private key is equal to the password stored in the memory then the locks open. In the unlikely event that we enter an unsolicited privacy statement, then Warning is turned on. For some with physical disabilities, even a basic job may require assistance. Auxiliary technology (AT) enhances the independence of people with disabilities by empowering them to perform tasks that they could not officially access. The current framework uses Open-CV apparatus to create python codes, and HAAR Course Calculation is sent. in a given image using the haar cascade algorithm. The Facial Landmark test algorithm is used for the formation of face keys and to detect detected face structure with specific link values (x, y). Eye movements are continuously monitored to detect the Gaze Ratio and based on the visual acuity the appropriate keyboard will be displayed. Then the blink rate will be calculated to update the appropriate character as a password. [4]

This paper [5] includes a real-time gaze-based PIN deployment application, visualization and tracking, and a smart camera to detect Morse PIN code. To overcome the existing limit, they have proposed a security system in two areas, one to verify the authenticity of the PIN using the Morine blinking PIN encryption, and another provides a secure alternative to the password. Receiving a blink of an eye with the Morse code, where the numbers are represented by points and dashes, which will be used to verify passwords and create a PIN is called blink-based authentication. Improving the custom PIN encryption by adding a Morse code-based PIN to provide an extra level of security is the main reason why this work. Morse code is one of the first forms of telecommunications, but today it is no longer used because of telecommunications. Since the proposed method [5] incorporates communication techniques with modern computer vision technology, the blink of an optical detection should be sufficient before the computer can detect 100% PIN recognition accuracy.

This paper [6] introduces a real-time system for pencil-based installation, eye recognition and pin detection using a smart camera. Gaze-based verification refers to the acquisition of an eye spot in all consecutive photo frames, as well as an eye tracking center over time. Password authentication will be done using Morse code, where the numbers will be represented as dots and dashes. Virtual security is about researching how security information should be managed in the system, both in the user interface and in the background, without losing consideration of resources and costs.Measuring usefulness and safety to achieve a positive outcome is defined by the principle of psychological acceptance. The proposed model contains a Graphical user interface (GUI) so that the user can interact with the system. Pygame or OpenCV can be used for this purpose. Facial Landmark Algorithm and Shape predictor are used to locate the eye reader by processing the Image. The first step is to identify the user's face accurately.The facial area mark algorithm is used for the purpose. After the face detection, it will try to find an eye within the area of interest. Webcam is used for taking high-resolution pixels. Even if one person has only one eye, it takes one eye to blink as an input.When a user blinks an eye, the system will take that input using the facial landmark algorithm and the weather forecast and rely on Morse code password setting and reset. password reset. To use a facial detector, a pre-trained model is required. This is a pre-trained model using shape_predictor_68_face_landmarks. 68 links can be visualized. [6] negotiated two-factor authentication, in which two layers of security were provided to verify the authenticity of the password. One uses visual-based authentication and the other uses mouse clicks for the purpose of converting letters or numbers into source code leading to improved security.

In this paper [7] The Author presents the new Light Password Verification Program (EGBP). The program is based on four basic ideas: system configuration, algorithm for recovering non-tracking students across all structures, allowing users to blink as region of a password and a unique way to recover user password using a built-in correction angle. EGBP has a few basic advantages compared to existing verification systems that include the need for an optical tracker that reduces system costs, eliminates speed measurement and requires minimal processing, and selects a higher length code that minimizes the chances of parallel password selection and increases security. The option of just memorizing a password is because the blink and instant fluctuation of a user is another advantage of this program. The suggested plan, the EGBP, is being offered, and the plan of the plan being presented includes two ideas. The algorithm for obtaining an adjustment and blinking will be established on tracking eye activities and there is no necessity to find a clear user point of view. The idea of a verification method is based on the angle created between the facts pulled from the proposed algorithm as a discipline method. Student location is received operating the Haar filtering method. In the next frame, the luxury, tracking is done with a Haar filter in 2D square near the student area in the previous frame. The pas sword rescue algorithm, after discovering the correction and maintaining it in the correction vector, is required to deliver an algorithm that determines the user's password. As mentioned earlier, a regular user point is not required. The main idea is at an angle between the composition from the present state to the following, and a built-in angle can oblige detect the hidden password. The system version test, 30 users, 15 men and 15 women, were invited to choose their passwords and enter them into the procedure to verify the password for 5 consecutive weeks. Each user was invited to experience in 5 categories. A new EGBP verification system, founded on eye movement research, is given, where, as with similar methods, learning the touch of each digit is not required. Failure to use commercial visual trackers and inferior system fees make it work on regular applications such as cell phones and filters.

In this paper [8], the algorithm for finding face and landmarks has been carefully integrated to provide automatic eye tracking, and has been accelerated to make the first important step in online testing, closed loop. Such tests have not yet been achieved and are expected to provide important insights into the functioning of emotional and psychological problems. Based on an extensive literature investigation, various algorithms for face detection and geographic designation have been studied and assessed. Two algorithms have been recognized as most appropriate for eyelid detection: Histogram-of-Oriented-Gradients (HOG) face detection algorithm and Ensemble-of-Regression-Trees (ERT) local marking algorithm. These two algorithms accelerate GPU and CPU, reaching speeds 1,753 × and 11 ×, respectively. To display the significance of the eyelid detection algorithm, an analysis hypothesis was formed and well-established neuroscientific research was used: blink detection. CNN reaches the highest points in memory (i.e., sensitivity) as it can detect 98.0% of the face inbound data. These models are known for their versatility and creativity.

In this Paper[9] ,the author evaluate three different eye gaze interaction methods for PIN-entry, all resistant against these common attacks and thus providing enhanced security. Besides the classical eye input methods we also investigate a new approach of gaze gestures and compare it to the well known classical gaze-interactions. The evaluation considers both security and usability aspects .Finally the author discuss possible enhancements for gaze gestures towards pattern based identification instead of number sequences. As author goal is a more secure but still usable solution, we set aside the potential advantages for the handicapped and also use interaction techniques that require button pressing and holding. Using these preconditions, the developed and adapted three possible interaction techniques (the traditional dwell time and look & shoot as well as the novel gaze gestures method).The standard eye-gaze interaction technique is the dwell time method. Here the user stares for a certain time (dwell time) at an area on the display to trigger an action. This dwell time is typically below 1000ms.look& shoot method, Here the user fixates an interaction object on the screen and simultaneously hits a button to trigger the action.

In this Paper [10] the author focuses on avoiding hot track attacks and licensing clients in order to pass on their password without the insanity of the viewer and create a framework for using the eye track gadget. As well as the security PIN, clients select PIN numbers with their eyes by simply focusing on the digits displayed on the screen. Because the target key is not used for the PIN corridor, no data about the entered digit is provided to the attacker by viewing it. The concept of eye tracking technology is used that continuously tracks human eye growth using a basic webcam and transmits insults as needed. The whole process can be divided into four categories, for example, facial recognition, eye recognition, the position of the illiterate person and eye contact as seen in the picture. This framework uses a USB or webcam to capture and disassemble client face enhancements.

The highlighted base and image base techniques are two different ways of identifying the face. Highlight based strategy: In this process, facial features are categorized, (for example, Nose, eyes, etc.), then assess their intelligence by looking at the location and the best ways to move away from each other. At the next eye, at this point the mouse starts to move away from its position. Slowly heats up its process and begins to work as indicated by eye development. The results of this study have been extremely valid for all implementation strategies. The standard error rate was 5 percent and the average length taken by each user to enter a password is 1 to 2min.

In recent years photo encryption has been suggested as a possible solution due to improved features and the ability to see and remember images. This paper introduces ImagePass image tracking tutorial, an image-based authentication method. The goal of the study was to determine how users perceived and responded to image verification. The author explores the usefulness of common elements by comparing visual patterns that appear with those found in other eye-tracking studies. The study outcomes show the blind places of visual sampling in the integrated visual interface and the probable differences between male and female users in visual image patterns. The writers examine whether eye correction can predict the place of passwords, while finishing that eye contact is not a reasonable forecast of passwords. [11]

This paper proposes a new algorithm, an algorithm for alignment, for tracking eye movements. Researchers are continuing to restore some of the functionality lost to disabled people using electric wheelchairs and powerful robots. This paper presents the use of an eye tracking method on these wheelchairs. Algorithm alignment follows eye movements to the left or right. The flashing feature is also used by the algorithm to control the start and position of the wheelchair. The system is tested in an extent equal to the area of the house. USB INTEX night vision camera connected to a cap worn by a user. The user-wearing cap has a light weight that only carries a small camera with LEDs. The user must turn left or right only to move the wheelchair to the selected location. Diagonal motion is achieved when the user only turns left or right for a quick term.[12]

In this project the writer constructed an Eye Dent system that presents an on-screen keyboard to the user, and allows the user to verify by looking at the characters in his password in documented order. By using the on-screen keyboard, we follow common password schemes, which can be used to rescue settings such as a private home or office. User-selected characters are specified using the default merging algorithm. The author has utilized EyeDent using the Eye Tech Digital Systems TM3 eye tracker [13]; this is a remote eye tracker real to 0.5 degrees that accepts head movement within a 25 x16 x 19 cm window. Before forming EyeDent, the author created an API cover in the form of a DLL that permits programs written in .NET languages such as C # to interact with the eye tracker using EyeTech's Quick Link API. The purpose of EyeDent is to provide users of eye tracking without the need for special triggers or predefined times.The author's initial results suggest that this goal can be achieved. Using Small Points Each of the 9 collections has led to many successful verification efforts by the authors. The author's results show that the flexible determination of the Minimum Points for Each Collection does not support the variability of stay, but more work is needed to adjust the algorithm to increase the level of validation.[13]

In this project, a smart camera, LabVIEW and considering software tools are used to develop eye detection and search algorithms. Algorithms are loaded onto a smart camera for processing images on the board. Eye detection means discovering the characteristics of the eye in one frame. Eye tracking is accomplished by finding the exact eye features in all multiple photo frames and connecting them to a specific eye. Algorithms are tested for eye detection and stalking beneath a mixture of situations including different face angles, head movement speed, and blindfolds to get your help on the proposed systems. This paper introduces the algorithms used and the performance results of these algorithms on the smart camera. Acquisition rate decreases as the independent level increases in all four test conditions under optimal conditions, with head movement, head angle on camera and slight closure of the eye area. Under ideal conditions when the face is directly in front of the camera, the visual acuity is over 93% even at the highest level of the frame.[14]

III. Conclusion

A major drawback such as forgetting your passwords and similar rewards can be overcome in this way and is a very similar safe option. The use of this technology will benefit all sectors of the corporate world. The applications of this method may be used for advanced security systems by performing additional improvements and advanced research In all experiments where subjects were sitting between 1 and 2 feet from the camera, it did not take more than three voluntarily. user blink before eyes are successfully detected. Another development is the compatibility of this program with inexpensive USB cameras, as opposed to a high-resolution CCD video camera. These Logitech USB cameras are very affordable and portable, and perhaps most importantly, support a maximum real-time frame of 30 frames per second. System reliability is demonstrated by the results of the high accuracy reported in the previous section.

References

[1]. Asha Rani K P, Asha K N2, Nidhi B Channappagoudar, Manonandan S K,Realtime Eye Tracking for Password Authentication IJERTV9IS100109 , Vol. 9 Issue 10, October-2020.

[2]. Dr. T R MuhiburRahman,Neha K, ReshmaM, Priyanka G , Pavitra V REAL TIME EYE TRACKING FOR PASSWORD AUTHENTICATION, Volume 11, No. 3, May-June 2020.

[3]. Indrajit Das, Ria Das, Shalini Singh, Amogh Banerjee, Md. GolamMohiuddin, AvirupChowdhuryDesign and Implementation of Eye Pupil Movement Based PIN Authentication System2020 IEEE VLSI Device, Circuit and System Conference (VLSI-DCS), 18-19 July, 2020, ED MSIT SBC.

[4]. Dr.A Syed Mustafa, Syed Zaid, SyedaZebaTabassum, TasmiyaBanu, UmmeAymun, Aparna Nair, Automated Eye Tracking Mechanism for Password Authentication, International Research Journal of Engineering and Technology (IRJET), Volume: 07 Issue: 08 | Aug 2020

[5]. Renuka N., Devaraju B. M., Morse code based Secured Authentication System uses Eye Blink through Haar Cascade and Facial Landmark Algorithm, International Journal of Advance Research, Ideas and Innovations in Technology, ISSN: 2454 -132X

[6]. Rajatha, SavitriKulkarni, Dr. Krishna A N, Gaze based Smart Eye Tracking System Password Verification, International Journal of New Scientific Research, Engineering and Technology (JIRSET), 1 January 2021.

[7]. HananehSalehifar, PeymanBayat, MojtabaAmiriMajd, blinking password: a new authentication system with high memorable and maximum password length,Multimedia Tools and Applications,02 January 2019.

[8]. Paul Bakker, Henk-Jan Boele, Zaid Al-Ars and Christos Strydis, Real-time face and landmark localization for eyeblink detection, arXiv:2006.00816v2 [cs.CV] 15 Jul 2020.

[9]. Alexander De Luca, Roman Weiss, Heiko Drewes, An eye-tracking security test to enter an Advanced PIN, Media Informatics Group Amalienstr, 2007.

[10]. Mrs.Pavitra S R,Mrs. Pushpalatha S, Eye tracking using Gaze PIN Password Verification, International Journal of Engineering and Technology Research (JERT),http://www.ijert.org ISSN: 2278-0181 Published by :www.ijert.org Vol. 9 Issue 06, June-2020.

[11]. Mihajlov Martin, TrpkovaMarija, ArsenovskiSime, Eye Tracking-based Graphical Authentication, Ss.Cyril and Methodius University Skopje, Macedonia .

[12]. Poonam S. Gajwani1 and Sharda A. Chhabria2, EYE FOLLOWING IN CONTROL OF THE SEAT, July-December 2010, Volume 2, No. 2, pages 185-187.

[13]. Justin Weaver, Kenrick Mock, BogdanHoanca, Gaze-Based Password Verification with Automatic Gaze Points, 2011 IEEE.

[14]. MehrubeMehrubeoglu, LinhManh Pham, Hung Thieu Le, RamchanderMuddu, and Dongseok Ryu, Real-Time Eye Tracking Using Smart Camera, 03 April 2012.

[15]. https://www.passportalmsp.com/blog/which-password-authentication-method-works-best-businesses