Journal of Informatics and Web Engineering

Vol. 2 No. 2 (September 2023) eISSN: 2821-370X

The Assistance of Eye Blink Detection for Two-Factor Authentication

Wei-Hoong Chuah[1], Siew-Chin Chong[2*], Lee-Ying Chong[3]

[1,2,3]Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Bukit Beruang, Melaka, Malaysia

**corresponding author: (chong.siew.chin@mmu.edu.my; ORCiD: 0000-0003-0421-4367)*

Abstract - This paper discusses the implementation of a blink detection method using 68 facial markers and the eye aspect ratio (EAR) to provide strong protection for access systems. It investigates the importance of 68 facial markers and explores how to use eye landmarks to calculate the eye aspect ratio. Access systems, which should have good security measures and be difficult to decipher, are typically safeguarded by passwords or multi-factor verification, such as passwords combined with facial recognition. However, these methods have inherent weaknesses, including the risk of shoulder surfing with passwords and the potential to be deceived by fake face images with facial recognition. To address these issues, a two-factor authentication method by using password with eye blink recognition is proposed as an effective solution for access control. By incorporating real-time eye blinking action, the system can avoid the use of fake images and prevent shoulder spoofing. To demonstrate the practical application of eye blink detection for enhanced two-factor authentication, a web application called "Eblink" is introduced. Functional tests have been conducted to validate the application's core features.

Keywords— Authentication Method, Eye Blink Detection, Facial Landmarks, Eye Aspect Ratio, Two-factor Authentication

Received: 07 July 2023; Accepted: 09 August 2023; Published: 16 September 2023

I. INTRODUCTION

Privacy, as the name implies, is information that a person does not want others to know or that others are not comfortable knowing. Privacy is the right of every human being, and it arose from the time when humans grabbed leaves to cover their shame. The sense of privacy is the first manifestation of natural man's entry into human society, and it should have arisen before human labor, that is, before primitive man was able to think abstractly, there was a similar awareness and feeling. In this era of rapid technological development, personal data will also be a kind of personal privacy that needs to be protected, because if personal data is not kept confidential, it can be misused or stolen, including the fact that criminals can use the stolen personal data to scam or harass users. Besides, watermarking is introduced to protect personal information such as personal pictures from tampering [1].

The first line of defense to protect users' privacy is the login username and password for each platform, website, or application. Most of today's password authentication services often mandate users to create complex passwords

Journal of Informatics and Web Engineering
https://doi.org/10.33093/jiwe.2023.2.2.8

Published by MMU Press. URL: https://journals.mmupress.com/jiwe

comprising a combination of letters, numbers, and special characters. However, this practice often poses a challenge for users to remember their passwords.

While the password with username authentication method remains one of the most prevalent login methods, it also suffers from certain drawbacks [2]. Firstly, it becomes challenging for users to detect and prevent someone from observing their password as they enter it, which can compromise security if someone is attempting to peek. Secondly, if multiple websites employ the same password and username combination, it significantly amplifies the risk and potential for user privacy data leakage. Not only that, but since password authentication schemes usually store passwords on servers, if a password list is accidentally leaked, the user's privacy will be compromised [2]. As far as blink detection is concerned, it is not secure enough to be used as an authentication tool on its own, but its real-time performance is effective in stopping the use of fake images and greatly reduces the risk of shoulder spoofing, so blink detection has the potential to be combined with other authentication methods. By combining blink with other authentication methods to form multi-factor authentication, the overall security of the authentication method can be improved by complementing each other. By requiring users to provide multiple forms of authentication, such as passwords, blink detection, and biometrics, systems can more effectively prevent unauthorized access to ensure the overall security of user privacy.

The main idea of this paper is to use eye blink detection to improve access security and use the eye blink as a secondary authentication factor for users. Today's applications are usually protected by passwords, biometrics, or two-factor authentication (e.g., password and OTP), but each of these methods has some drawbacks, such as the risk of shoulder surfing with password authentication, the possibility of being spoofed by fake facial images with facial recognition, and the need for the user to perform additional operations on the mobile device with the password and OTP authentication code. This web application uses a two-factor authentication method using a password with eye blink count recognition as the login method. This web application utilizes a two-factor authentication approach combining a password with eye blink count recognition as the login method. This method offers a user-friendly yet highly secure means of accessing the system. When blink detection is combined with other authentication methods (e.g., passwords, face detection), these methods complement each other well and provide stronger protection for the user.

The paper is structured into various sections, each serving a distinct purpose. Section II comprises a comprehensive literature review of the relevant technology pertaining to eye blink detection. Building upon this knowledge, Section III elucidates the proposed implementation, providing an in-depth technical explanation. Section IV showcases the development of the web application, highlighting its integration with real-time eye blink detection. Section V delves into the user acceptance tests conducted, analyzing the system's performance across different scenarios. Lastly, in Section VI, the paper concludes, summarizing the findings and drawing final remarks.

II. LITERATURE REVIEW

A. The Use of Eye Blink Detection

Eye blinking is an unconscious biological characteristic, and generally healthy people blink at intervals of 2s to 10s, with eye closure durations of 100ms to 400ms [4]. using the unconscious blink frequency of healthy people, blink systems are mainly used in two scenarios, such as fatigue detection and in vivo detection.

Conscious blinking, or voluntary blinking [4], refers to the conscious and purposeful act of blinking. It involves utilizing all the relevant muscles [5] and being fully present and engaged in the blinking behavior, rather than an automatic or unconscious reflex. On the other hand, it can be used as an interactive system for special occasions or special populations.

B. Driver Monitoring Systems for Detecting Driver Fatigue

Fatigue is one of the most common causes of traffic accidents [6], and the fatigue rate is so high that it is necessary to prevent accidents caused by drowsiness. One of the things that can prevent this is a Driver Monitoring Systems (DMS), and blink detection is also used in this technology.

Blink detection is used in a DMS based on visual sensors to detect driver status indicators. Human beings have distinct facial expressions or characteristics when they are tired or tired, such as more frequent blinking, longer blink durations, or even the absence of blinking because they are asleep, and these actions are very useful as a basis for judgment.

C. In Vivo Detection Assistance for Face Recognition

With the development of these technologies, the application of face recognition technology is becoming more and more widespread, but also with the development of technology is the increasing security risks. Some images from movies and films are slowly becoming reality, and unsuspecting people can easily pass face recognition by putting on a photo or mask prepared in advance to disguise themselves as other people. As the risks and pitfalls of such face forgery increase day by day, in vivo detection (liveness detection) technology is gaining more and more attention.

Liveness detection technology is used to identify whether the object detected by the imaging device is a real live object and not a fake or dead object with no vital signs. Face recognition live detection systems [7] use relatively secure biometric features combined with pattern recognition-based face recognition to combat face forgery attacks. Live detection techniques are usually classified into three categories, namely 8 picture-based live detection, collocated live detection and silent live detection. Blinking is used in cooperative live detection, where the user is prompted to perform a corresponding action to verify that a live body is operating.

D. Conscious Blinking Interaction System

With the development of mobile devices, the human-machine interaction between users and devices is getting richer and richer. At present, there are two main types of human-device interaction methods: one is button-based, in which commands are issued through buttons; the other is touch-based, in which the touch screen is capacitive or resistive, and users issue commands by touching the screen with their fingers. These two ways are based on human-computer interaction, which requires the intervention of the hands, when the hands are occupied, it is impossible to complete the interaction between people and equipment, so it cannot be applied to some special occasions, or some disabled people.

However, with the development of technology, new interaction methods are emerging, especially a variety of non-contact operation methods, mainly voice control such as voice-controlled wheelchair [8], voice-controlled e-commerce applications [9] and somatosensory control such as Virtual Reality (VR) gloves [10], wearable health devices, and eye blink detection is one of the interaction methods based on somatosensory operation. In eye blink interaction, the recognition algorithm can identify the facial action of blinking and distinguish whether the received blink signal is a conscious blink by the interactor.

E. Traditional Password Authentication

As a first line of defense against unauthorized access to personal information, a password is a secret combination of user-defined characters that can be used to identify the user and authorize access to specific devices or websites according to the user's needs. Passwords are generally used in combination with a user-defined username, email address or cell phone number. The more complex and stronger the password, the more effective it is in protecting the user's account, and most password 9 authentication services today require the user to use a password that includes letters, numbers and also special characters.

F. QR code Authentication

The full name of QR code is Quick Response Matrix Code. It is a type of two-dimensional barcode, which is widely used in cell phone code reading operations. QR codes are faster to read and have greater data storage capacity than ordinary 1D barcodes, and do not require straight alignment with the scanner as 1D barcodes do. QR code authentication is a phone-as-token authentication [11], the essence of QR code authentication is that the requesting party, which is the web side, requests the logged-in party, which is the mobile side, to write the login credentials into

a specific medium (QR code) by scanning it for authentication. In this process, the QR code acts as a bridge between the requesting party and the logged-in party.

G. Biometrics Authentication

Biometrics is a technology that uses the inherent physiological characteristics or behavioral features of the human body to identify individuals. Biometrics technology collects biometric features by sampling them through computers, sensors and biometrics, extracts the unique features, and converts them into digital codes through digital processing and then combines the codes into feature templates in the database. When a user interacts with the recognition system, the recognition system acquires feature data that will be compared with the feature templates in the database to confirm whether the interactors match and thus determine the identity of the user.

Compared to other biometrics recognition technologies, facial recognition based on facial features is more easily used in web-based authentication because it only requires a camera or a webcam to capture, detect and recognize the user's face [12].

H. Two-Factor Authentication

Two-factor authentication [13], or 2FA for short, is an authentication method that requires users to provide two identity credentials to prove their identity in order to gain access. Two-factor authentication combines two of the three elements used in cryptography for authentication (authentication content that needs to be remembered by the user, the user's possession of authentication hardware, and the user's own unique characteristics) to achieve dual-factor authentication. Two-factor authentication can be very effective in improving the security of system access control because all three elements of authentication have weaknesses when used independently and combining the two elements allows the two elements to complement each other. Two-factor authentication can work in a number of ways. One of the most common examples of 2FA is password authentication coupled with OTP authentication.

I. Comparison between Existing Authentication Methods

Each authentication method protects the user's privacy or personal data as the method used to authenticate the user. Facial authentication is unique compared to the other authentication methods because the features of the face are difficult to replicate with current technology. Compared to authentication methods that require a 23 password, QR code and facial authentication are more user-friendly as they do not require a password to log in, while compared to other two-factor authentication methods that require the use of a mobile device for assistance, the two-factor authentication combination of password and blink count eliminates the need for users to operate an additional mobile device when logging in. Authentication methods that use mobile applications or OTP information as a secondary authentication factor can notify the account holder when someone tries to authenticate. The other methods are more difficult to crack than simply using a password for authentication.

III. IMPLEMENTATION OF THE PROPOSED SOLUTION

The objective of this project is to create a web-based application that employs a dual authentication mechanism for login. The first authentication layer involves the traditional password and username combination. As a second layer of authentication, the application utilizes eye blink detection. Blinking has some advantages over the other second authentication factors, as blinking does not require the user to manipulate the mobile device additionally, thus increasing user-friendliness, and blink detection is a real-time action that avoids the risk of being spoofed by a fake facial image, compared to facial recognition. In order to enhance the security of the login authentication process, this project implements a blink detection system that goes beyond simple blink detection. During the registration phase, users will be prompted to pre-record the specific number of blinks required for login authentication. This recorded number of blinks will then be utilized during the login process to authenticate the user. As a result, a key aspect of this project revolves around accurately calculating and determining the appropriate number of blinks that each user can employ for successful authentication.

In this proposed implementation, the 68 face landmarks and Eye Aspect Ratio (EAR) have been used to determine if a person is blinking or not. The process for detecting blinks is illustrated in Figure 1. Firstly, it checks for a new frame, and if there is none, the detection process ends. If a new frame is available, it proceeds to check for the presence of a face. Once the face is detected, the landmarks of the eyes within the face are extracted, and these detected points are used to calculate the vertical and horizontal lines of the eyes for EAR computation. Finally, based on the calculated ratio, it determines whether a person is blinking or not.

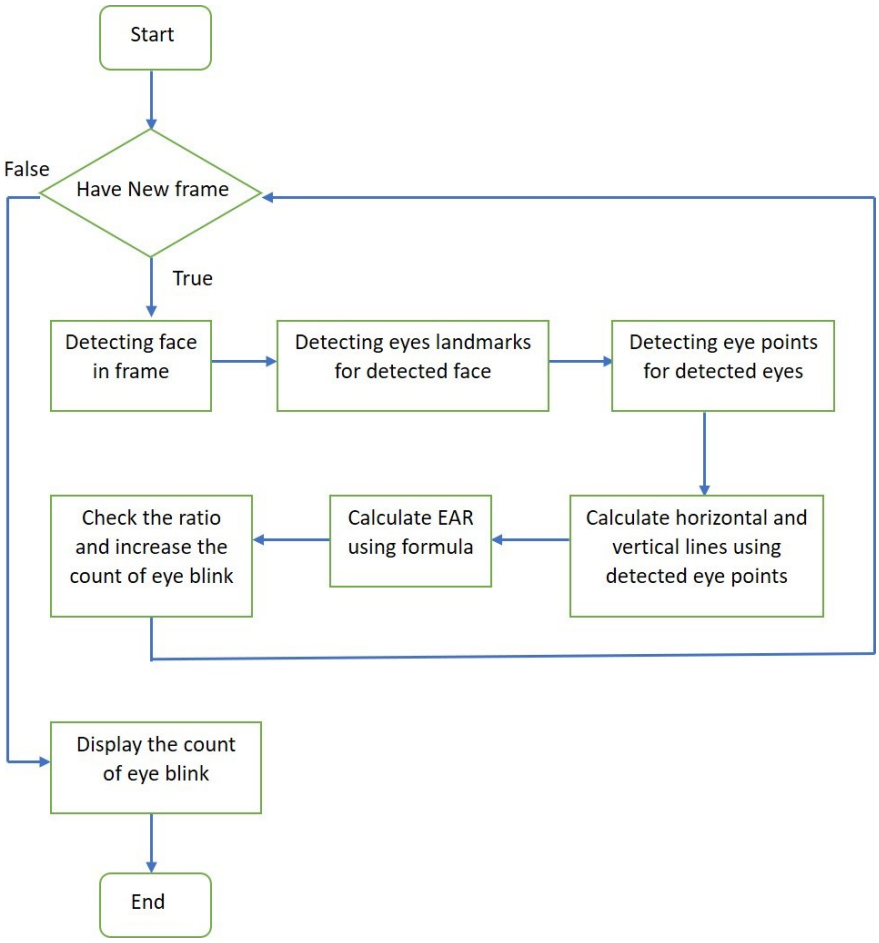


Figure 1. Flowchart Of The Eye Blink Detection

A. 68 Facial Landmarks

The '68 face landmarks' is a set of the points on human face that used for face landmark detection, as shown in Figure 2. These landmarks are often used for tasks in computer vision or machine learning application such as face identification, facial expression analysis, and facial feature tracking.

These 68 facial landmarks provide information about the shape and structure of the face and can be used to compute facial attributes such as the location of facial organs (such as eyes, nose, and mouth) and the degree of eye or mouth opening. These computed facial actions can be used for facial expression analysis and facial pose estimation applications.

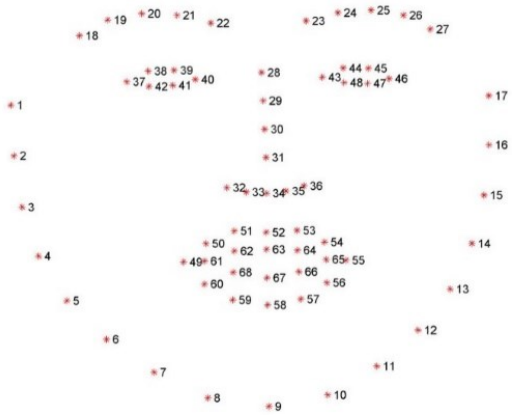


Figure 2. 68 Face Landmarks

B. Eye Aspect Ratio (EAR)

Eye Aspect Ratio (EAR) is an important factor used to determine whether a person blinks or not [14]. EAR calculates the horizontal line (width of the eye) and the vertical line (height of the eye) by using landmarks of both eyes, and since the width of the eye will be a constant and the height of the eye will vary depending on the opening and closing of the eye, we can detect whether a person blinks by calculating the ratio between them (open eyes when the ratio is approximately constant, and closed eyes when it decreases rapidly). Figure 3 shows the EAR calculation.

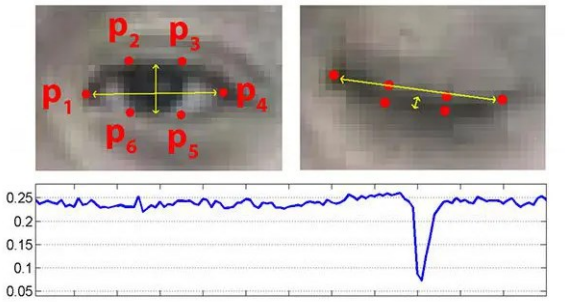


Figure 3. Top: The Open And Close Eye Landmarks, Bottom: Graph Of Eye Aspect Ratio Over Time With A Significant Decrease Indicating Blinking Occurred [14].

Equation 1 shows the formula for calculating EAR, where P1, P2, P3, P4, P5, and P6 represent the landmarks of the eyes. |P2-P6|+|P3-P5| is used to calculate the average vertical distance between the two eyes, while 2|P1-P4| is used to normalize the measurements to ensure consistent EAR values across different faces.

$$EAR = \frac{|P2-P6|+|P3-P5|}{2|P1-P4|} \quad (1)$$

Figure 4 shows how to use Python code to calculate EAR. The code will receive the coordinates of the eye region to calculate the vertical and horizontal lines of the eye and compute the value of EAR

```
def eye_aspect_ratio(eye):
    A = np.linalg.norm(eye[1] - eye[5])
    B = np.linalg.norm(eye[2] - eye[4])
    C = np.linalg.norm(eye[0] - eye[3])
    ear = (A + B) / (2.0 * C)
    return ear
```

Figure 4. Python Code For Calculate EAR

The Python code in Figure 5 is performing eye blink detection by using EAR. The code will first preset the EAR threshold, the consecutive frames threshold, the counter to record the number of consecutive closed eyes frames, and the total number of blinks to 0.2, 1, 0, and 0.

Next, the code will initialize the face detector and facial landmark predictor from the dlib library and use shape_predictor_68_face_landmarks.dat as the predictor model. After that, the code will extract the landmarks for the left and right eyes.

After the preset work is done, the code will then read the frames of the video stream one by one through a loop and process them. The frames are resized to 450 pixels and are gray scaled. The code will use the face detector to detect face regions on the processed grayscale images and return a list of detected rectangular boxes.

Next, a facial landmark predictor is applied to obtain the coordinates of the landmark on the detected face. It then extracts the corresponding landmark coordinates based on the indices of the left eye and right eye landmark and passes them to the eye_aspect_ratio function, as shown in Figure 4, to calculate the EAR.

If the calculated EAR is less than the preset threshold (0.2), the counter will increase; while if the counter is greater than or equal to consecutive frames threshold (1), the TOTAL will increase. The latter case represents that a complete blink has been detected, and the counter will be reset to 0. The loop will continue until the end of the video stream or until there are no more readable frames. At the end of the video, the code will print the total number of blinks and send the total number of blinks back to the Laravel backend for further processing.

In summary, the Eblink web application utilized Laravel for its back-end development, enabling the implementation of features like login and registration. JavaScript was employed for front-end development, encompassing the user interface and interactive components. Python was utilized to implement the blink detection feature, which added an extra layer of authentication. MySQL was chosen as the database management system, facilitating the storage of user profiles and sensitive information provided by users, ensuring data persistence and security.

```python
def blink_detection(video_path):
    vs = FileVideoStream(video_path).start()
    file_stream = True
    EYE_AR_THRESH = 0.2
    EYE_AR_CONSEC_FRAMES = 1
    COUNTER = 0
    TOTAL = 0
    detector = dlib.get_frontal_face_detector()
    predictor = dlib.shape_predictor("shape_predictor_68_face_landmarks.dat")
    (lStart, lEnd) = face_utils.FACIAL_LANDMARKS_IDXS["left_eye"]
    (rStart, rEnd) = face_utils.FACIAL_LANDMARKS_IDXS["right_eye"]

    while True:
        if file_stream and not vs.more():
            break

        frame = vs.read()
        if frame is not None:
            frame = imutils.resize(frame, width=450)
            gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
            rects = detector(gray, 0)

            for rect in rects:
                shape = predictor(gray, rect)
                shape = face_utils.shape_to_np(shape)

                left_eye = shape[lStart:lEnd]
                right_eye = shape[rStart:rEnd]
                left_ear = eye_aspect_ratio(left_eye)
                right_ear = eye_aspect_ratio(right_eye)
                ear = (left_ear + right_ear) / 2.0

                if ear < EYE_AR_THRESH:
                    COUNTER += 1
                else:
                    if COUNTER >= EYE_AR_CONSEC_FRAMES:
                        TOTAL += 1
                    COUNTER = 0
```

Figure 5. Python Code For Eye Blink Detection

IV. PROPOSED WEB-APPLICATION - Eblink

In this paper, a proposed web application, named Eblink has been provided to demonstrate the assistance of eye blink detection for two-factor authentication. The web application has applied two-factor authentication method that combines a password and uses blink detection as a second authentication factor. Figure 6 shows the login function of the proposed web-application “Eblink”. After the registered email address and correct password have been entered, the user will be redirected to an eye blink check page, as illustrated in Figure 7, for the second factor authentication, which is eye blink detection.

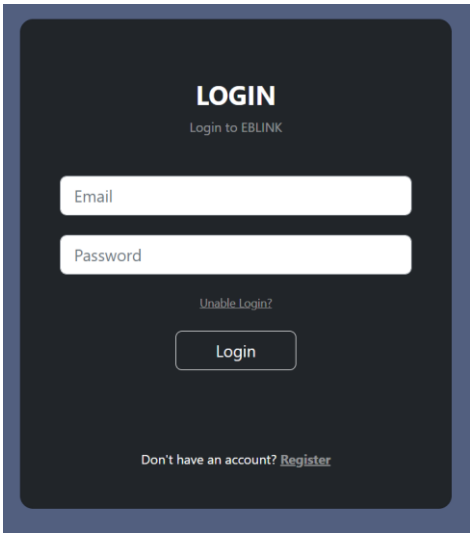
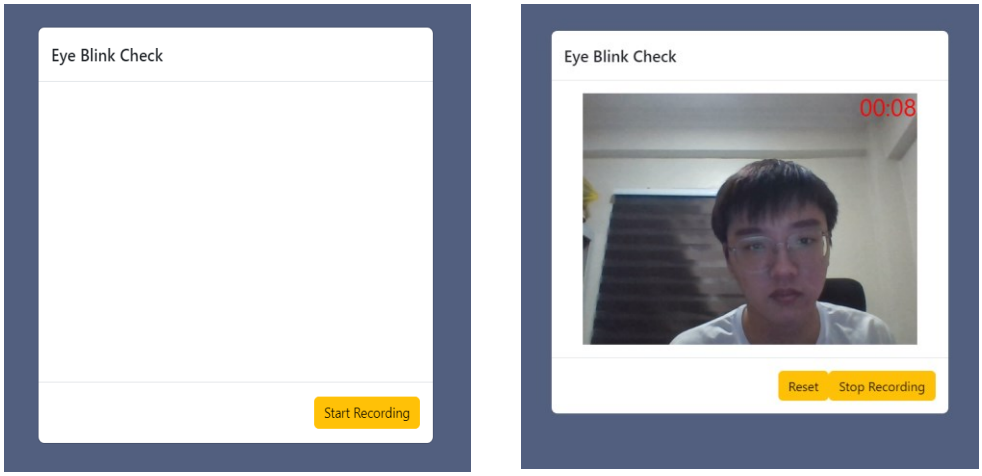


Figure 6. Login Page For Eblink



(a) (b)

Figure 7. (a) Start Recording Page For Capturing Eye Blink Video, (b) Stop Recording Page To Stop Eye Blink Capturing.

In the eye blink check page, user need to click the Start Recording button to record their blinking video and click "Stop Recording" after they have finished recording. After the recording is stopped, a preview record video will be displayed to allow for video checking. The "Reset" button allows user to re-record the video if they are dissatisfied with the video. After checking the preview record video, user can click the "Upload Video" button to submit their recorded video to the backend for further processing. If user blink's count doesn't match with the database, user will be redirected to the login page with an alert, as illustrated in Figure 8.

Figure 8. Blink Detection Failure Alert

In addition to utilizing blink detection for login authentication, Eblink extends its usage to safeguard sensitive user information such as login credentials, card details, identity information, and secret notes. To prevent data leakage, these pieces of information are encrypted. When users wish to access the encrypted information, they are required to unlock it using eye blink detection. Only a valid count of eye blinks is accepted to successfully unlock and view the information. This additional layer of protection ensures that unauthorized individuals cannot access the sensitive data stored within the Eblink application. Figure 9 and Figure 10 show the details of information before and after unlocking.

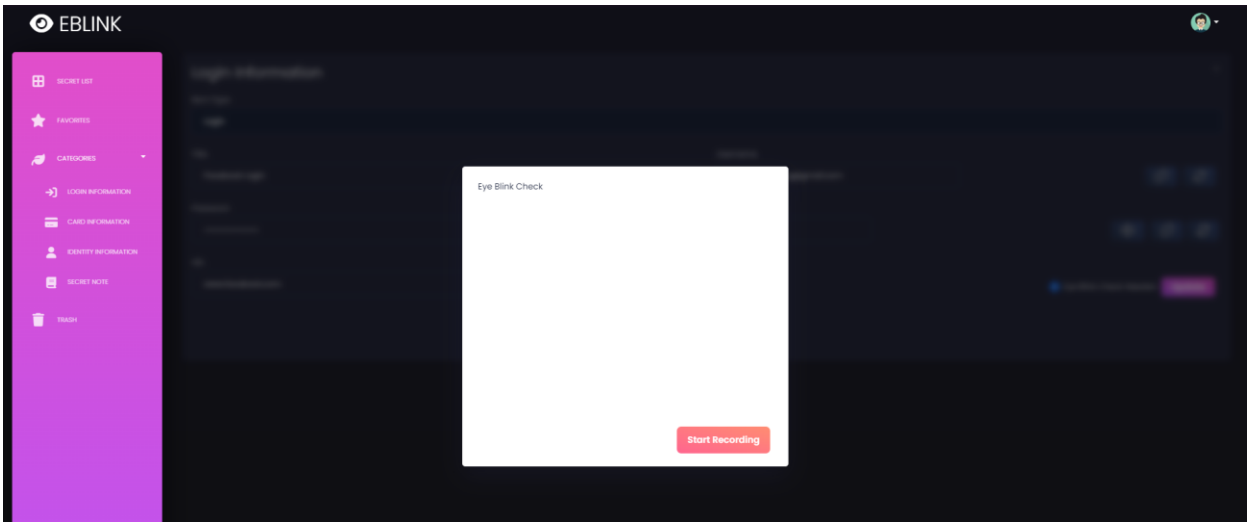


Figure 9. Information Details Page Before Unlocking

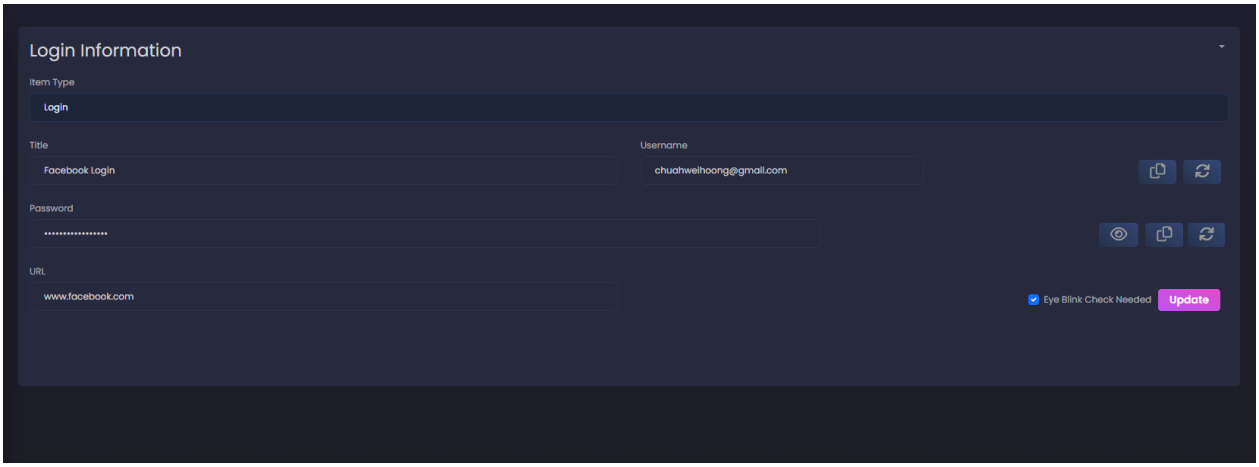


Figure 10. Information Details Page After Unlocking

During testing, it was observed that the camera used for blink detection has a frame rate limitation. Consequently, if the blink rate is excessively rapid, the camera may miss fast blinks occurring between consecutive frames. This poses a challenge because the implemented code relies on the eye aspect ratio (EAR) threshold to determine the eye state (open or closed). As a result, fast blinks might cause the eye to remain closed for the specified number of consecutive frames, leading to undetected blinks. Additionally, reflections from glasses can introduce errors in the measurement of the eye contour, potentially impacting the accuracy of the calculations and the detection of the number of blinks.

V. USER ACCEPTANCE TEST

This section discusses the testing of the functionalities of the Eblink application and compares the expected performance with the actual performance of the application. The purpose of testing the Eblink application is not only

to evaluate its effectiveness but also to identify and fix any potential bugs in the application in advance. Table 1 shows the results of the functional tests related to the eye blink function in the Eblink application. From the various test cases, the functional tests validate that the application's core features especially the eye blink detection is performing well.

Table 1. User Acceptance Test Cases of Eye Blink Function

No	Test Cases	Expected Outcome	Actual Output
1	Eye Blink detection at register page	Users can open the eye blink detection modal by clicking on the eye blink button and input the number of eye blinks by uploading a video.	success
2	Eye Blink Check	After successful password authentication, users will be redirected to the eye blink detection page for a second round of authentication.	success
3	Number of eye blink detected is incorrect for the login	User will be redirect back to the login page and an alert of incorrect eye blink message will pop-up	success
4	Reset password	Users can reset their password and update their eye blink settings. They will have the option to enter a new password and adjust their eye blink preferences.	success
5	View encrypted information	The encrypted information details will be blurred, and an eye blink detection modal will appear.	success
6	Eye blink verify for encrypted information	Users can complete the eye blink detection by using the eye blink detection modal. Once the verification is successfully completed, the details will be displayed.	success

A pre- and post-development questionnaire was administered to a group of 66 users in order to gather their input, feedback, and requirements for the software under development. The questionnaire specifically focused on obtaining respondents' perspectives on various certification methods and their opinions on the incorporation of blinking as a secondary certification method. The primary goal of the questionnaire was to gather valuable insights and viewpoints from the users, thereby informing the development process and ensuring that user needs, and preferences are considered.

Based on the analysis of the questionnaire, it was found that the dual authentication method combining passwords with other authentication factors received significant popularity and positive user feedback. This highlights that while password authentication alone may not be flawless, it can be highly effective when used in conjunction with other authentication factors. Notably, 66% of the respondents expressed their interest in utilizing blink detection as a second authentication factor, indicating a potential market for blink detection authentication. Furthermore, 74% and 72% of the participants expressed their belief that using blink detection as a second authentication factor would enhance both security and convenience respectively.

VI. CONCLUSION

This paper presents an implementation of blink detection using 68 facial markers and the Eye Aspect Ratio (EAR) technique. It emphasizes the significance of 68 facial markers in facial feature tracking and various computer vision applications. The paper explains the rationale behind employing the eye aspect ratio (EAR) for blink detection and elaborates on the calculation process. Moreover, the paper introduces Eblink, a web application that exemplifies the utilization of blink detection to strengthen two-factor authentication. By combining traditional password authentication with eye blink detection, Eblink enhances the security of user authentication, guarding against shoulder spoofing and fake face authentication. Comprehensive user acceptance tests were conducted, and the performance results obtained were found to be highly satisfactory. The tests involved assessing various aspects of the system, including functionality, usability, security, and performance. Users actively engaged with the system and provided feedback on their experience. The performance of the system met or exceeded the defined criteria, demonstrating its

effectiveness and reliability. These positive outcomes from the user acceptance tests affirm the successful development and implementation of the system, ensuring its readiness for deployment and usage. Looking ahead, the field of eye blink detection technology is expected to progress further, uncovering novel applications across various domains. Future advancements may involve more accurate and robust blink detection algorithms capable of identifying diverse blinking patterns and eye states, thereby enhancing the precision and dependability of eye blink-based authentication systems.

ACKNOWLEDGEMENT

This research work was supported by a Multimedia University, Faculty of Information Science and Technology through the Final Year Project and the authors received no funding from any party for the research and publication of this article.

REFERENCES

[1] W. Jing, L. W. Ang, S. Palaniappan, B. He, "Robust Image Watermarking With Quaternion Fractional-Order Polar Harmonic-Fourier Moments Based On Wavelet Transformation: Resistance Against Rotation Attacks," Journal of Informatics and Web Engineering, vol. 2, no. 1, pp. 56 – 65, 2023.
[2] W-Chi. Ku, "Weaknesses and drawbacks of a password authentication scheme using neural networks for multiserver architecture", IEEE Transactions on Neural Networks, vol. 16, no. 4, pp. 1002–1005, 2005, doi: 10.1109/TNN.2005.849781.
[3] A. A. Abusharha, "Changes in blink rate and ocular symptoms during different reading tasks. Clinical Optometry", Clinical Optometry, vol. 9, pp. 133–138, 2017.
[4] K. Kwon, R. J. Shipley, M. Edirisinghe, D. G. Ezra, G. Rose, S. M. Best, R. E. Cameron, "High-speed camera characterization of voluntary eye blinking kinematics," Journal of the Royal Society Interface, vol. 10, no. 85, 2013.
[5] "Why Do We Blink Our Eyes? | MyVision.org", 2023. https://myvision.org/eye-health/why-do-we-blink/
[6] N. A. C. Hasan, K. Karuppiah, N. A. Hamzah and S. B. M. Tamrin, "Risk Factors of Fatigue: A Systematic Review Among Transportation Drivers," Malaysian Journal of Medicine and Health Sciences, vol. 17, pp. 184-192, 2021.
[7] H. Jee, S. Jung, J. Yoo, "Liveness Detection for Embedded Face Recognition System," International Journal of Biological and Medical Sciences. vol. 1, pp. 235-238, 2006.
[8] R. J. Simpson, S. P. Levine, "Voice control of a powered wheelchair", IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 10, pp. 122–125, 2022.
[9] M. S. Kandhari, F. Zulkemine, H. Isah, "A Voice Controlled E-Commerce Web Application", 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, pp. 118-124, 2018.
[10] J. Perret, E. V. Poorten, "Touching Virtual Reality: A Review of Haptic Gloves", 16th International Conference on New Actuators, pp. 1–5, 2018.
[11] A. Abbas, "QR Code in Authentication Services: A Safe and Secure Verification Process", 2023. https://www.linkedin.com/pulse/qr-code-authentication-services-safe-secure-process-aliasgar-abbas
[12] P. I. Fatema, A. Khan, A. Gedekar, A. Khawaja, M. Barghat. N. Khan, "Masked Face Recognition," International Journal of Advanced Research in Science, Communication and Technology, pp. 98–102, 2021.
[13] Q. Wang and D. Wang, "Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices", IEEE Transactions on Information Forensics and Security, vol. 18, pp. 597-612, 2023.
[14] T. Soukupova and J. Cech, "Real-Time Eye Blink Detection using Facial Landmarks", 21st Computer Vision Winter Workshop, 2016.