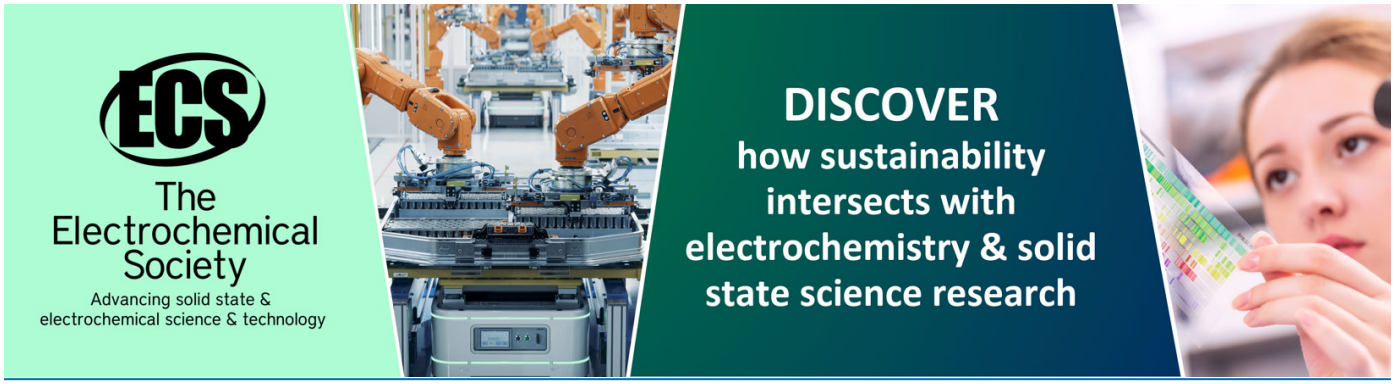
“LOOK & BLINK” TWO STEP VERIFICATION SECURITY LOG IN SYSTEM



"LOOK & BLINK" TWO STEP VERIFICATION SECURITY LOG IN SYSTEM

Liang Kai Qi[1], Razaidi Hussin[1], Afzan Kamarudin[1], Rizalafande Che Ismail[1, 2], Mohd Nazrin Md Isa[1] and Siti Zarina Md Naziri[1]

[1]School of Microelectronic Engineering, Universiti Malaysia Perlis, Kampus Pauh Putra, 02600 Arau, Perlis, Malaysia.
[2]Faculty of Computing and Informatics, Albukhary International University, Alor Setar Kedah, Malaysia.

Email: imkaiqii@gmail.com

Abstract. A new artificial intelligence security design which is face recognition with eye blinking login system is proposed. It aims to strengthen the security account for each user using artificial intelligence technology and increase speed and user convenience for security during login. The face of a person cannot be copied and it can replace the username of the user, while eye blinking detection is another step for double verification replacing the password of a user. It is a two-step verification process that can be applied to all sorts of account login field so that this technology can replace the old school username with a password security system. The recognition system used a real-time where it is reducing the number of hackers in the field as it is impossible to hack a person's real-time face. The proposed system has been tested and analyzed the functionality by accessing the personal account in the university's portal.

1. Introduction

This project is to propose a new two-step verification for the security system for every user of any system. With this new security system, it can reduce the time used to key in every account's username and password to log in to the system which will increase the speed of logging into online accounts especially for business accounts. Besides that, this security verification can increase security by using the owner's face as the username of the account as each person's face are unique and almost impossible to be hacked. Furthermore, it also increases the security by adding a blinking procedure after the face recognition to confirm the person is a real-time user instead of a robot or picture. For example, the owner of the account must first be identified and verified by the database of the system before proceeding to the eye blinking procedure. By surpassing both of the verification steps, only the person can log in to their accounts into the system such as bank accounts or company accounts or more.

2. Methodology

In this project, Python and Open CV are used to perform the coding and simulation. The security verification system is separated unto three parts; which is face recognition, eye blinking, and account logging in.

2.1. Face Recognition

Face recognition is a recognition method used to identify faces and appearance of human individuals whose images are saved in the data set. [1] It has become one of the very highly demanded applications in the last two decades, mostly due to the new artificial intelligence technologies developed and the high quality of the current videos and cameras in our daily lives. [2] Face recognition from an image or video is processed by extracting, crop, and resized the facial images, and then it is converted to a grayscale image. [3] The face recognition algorithm is in charge of searching for characteristics which is the best pair to the image. [4] The face recognition systems can operate basically in two modes, which are known as verification or validation of a human facial image and identification or facial recognition. For verification or validation of a human facial image, it mainly matches the input of the facial image with the facial image connected to the user which requires the authentication. It can be said as a principally 1x1 comparison between images. While for the identification or facial recognition, it mainly matches the input of a facial image with all the facial images from a dataset with the main reason to search the user that matches that face. It can be described as a 1xN comparison. There are several types of face recognition algorithm. For this project, Open CV face recognition is used as illustrated in Fig 1. Deep learning is also used to apply face detection, which detects the presence and location of a face in an image, but does not identify it. It also used to extract the 128-d feature vectors which are called embedding that quantifies each face in an image.

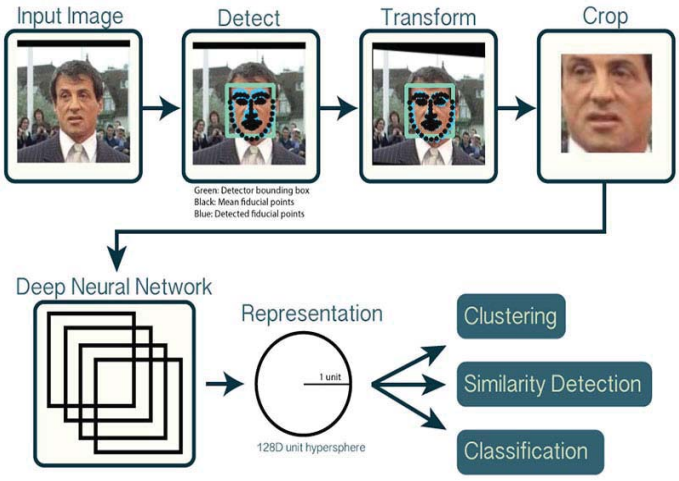


Fig. 1 shows the flow chart of Open CV face recognition algorithm [5]. OpenCV is used to facilitate face recognition. By using deep learning and OpenCV together, it can detect faces, compute 128-d face embeddings to quantify a face, train a Support Vector Machine (SVM) on top of the embeddings and then recognize faces in images and video streams.

2.2. Eye Blink Detection

By using facial landmarks to detect significant parts of the face, including eyes, eyebrows, nose, ears, and mouth, this also indicates that it can extract particular facial structures by determining the indexes of the particular face parts.

Because of only focusing on blink detection, two groups of facial structures which are the eyes play the most important role of all. Each of the eyes is represented by 6 (x, y)-coordinates, which begins from the left corner of the eye and then waging clockwise around the remainder of the region of the eyes. [6]

This project requires a formula named as the Eye Abstract Ratio formula to detect the difference of the eye landmarks when the eye is wide open and tightly closed. The concept of the EAR is illustrated in Fig. 2. [7-8] When the eye is wide open, the EAR will be approximately in constant value, when the eye is closed, the EAR will drop sharply and there is when it detects a blinking effect. While in Fig. 3 shows the difference value of EAR when the eye is in blinking condition or not.

$$\mathrm{EAR} = \frac{\|p_2 - p_6\| + \|p_3 - p_5\|}{2\|p_1 - p_4\|}$$

Fig. 2 shows the formula of the EAR for Eye Blinking Detection [9]. P2 and P3 is the upper eye arch, P1 and P4 is the side of the eye, P6 and P5 is the lower eye arch.

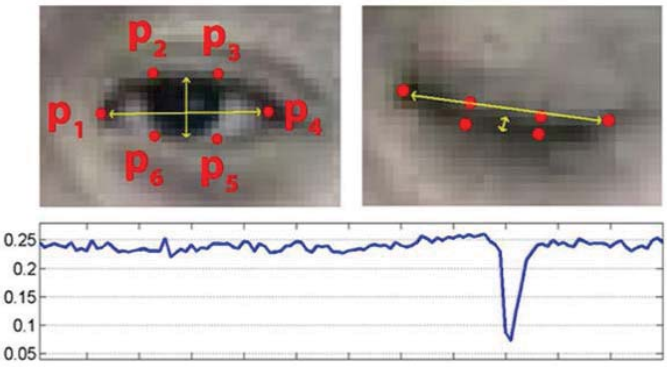


Fig. 3 shows the simulation graph of the EAR formula for Eye Blinking Detection [9]. When the eye is wide open, the EAR value is high and constant. Once the eye is shut when a blink occurs, the EAR value will drop instantly to a low value and it will rise back to the higher value when the eye is back open. This will indicate a blink happens and the blink count will count to 1.

2.3. Automated Login System

In this project, our university's portal webpage which is the UniMAP portal is used to perform the logging in after an eye blinking detection is determined. Fig 4 shows the webpage that will be used for testing purpose. The security system design allows automating login to the owner's account in the university portal. A type of third-party library named Selenium is needed to be applied to operate this purpose. [10]

The Python script is edited to assign the specific customized website page URL which is the university portal webpage and the username with the password of the person of the owner. After saving the username and password database of the page source into the script, the auto login system will be performed every time the two-step verification is surpassed.

Fig. 4 shows the login webpage for the university's portal. Once both of the face recognition and eye blinking verification step is done, the owner's ID and password will be automatically key in into the blank space and it will auto login into the personal account.

3. Results

3.1. Face Recognition

The results for face recognition are showed in Fig. 5. Real-time face recognition comprises face detection from a series of frames from a video- capturing device. The area of the frame that is different can be identified and the individual detected is label on top of the frame box.

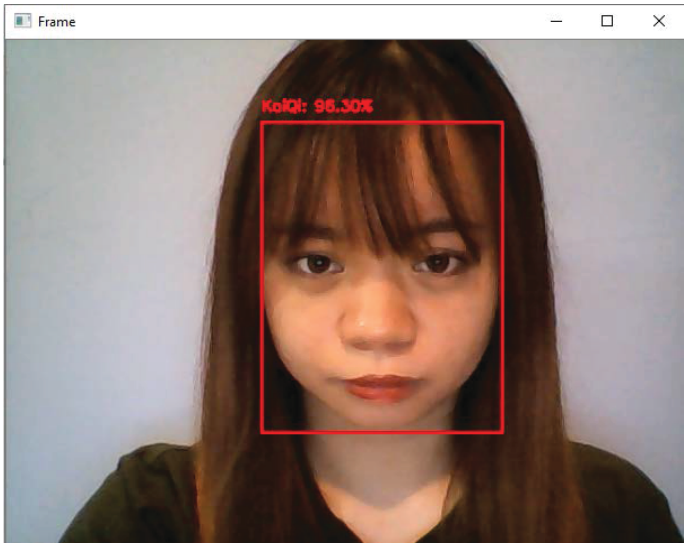


Fig. 5 shows the results of face recognition of the first verification step of the system. The name of the owner "Kai Qi" and the percentage of accuracy is shown in the frame.

However, if the person blocks their face from the real-time webcam, the design will not detect any faces or label any predicted names on the frame box as the person in front of the camera is not identified properly. This can be the same as applying glasses, books, accessories, and more. Thus, there is no face

detected within the camera and there is no person identified and predicted from the design. Fig. 6 shows the example of an unidentified face due to obstacles covered the face.

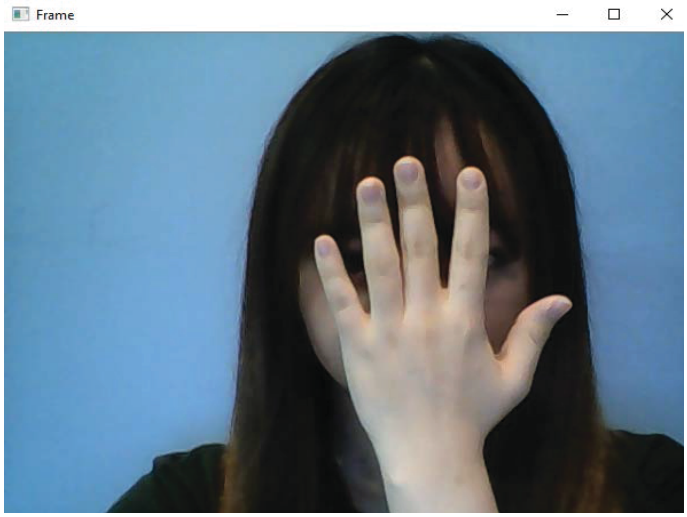


Fig. 6 shows the face is being covered or blocked with obstacles, the face recognition will not be able to detect any faces saved in the database.

3.2. Eye Blink Detection

Facial landmarks for eye blinking detection is been implemented and add inside the design. In terms of theory, the facial landmarks for both eyes are detected, the eye aspect ratio is computed for each eye, which gives us a singular value, relating the distances between the vertical eye landmark points to the distances between the horizontal landmark points. The value of the EAR is used to determine whether the person is blinking or not. The EAR ratio will remain constant when the eyes are open. If the person closed the eye, the EAR will rapidly approach zero. Thus, the value of constant and approaching zero is used in determining the person is blinking the eyes. Fig. 7 shows the EAR value during the initial stage or before blinking the eyes. Based on the width and height of the eye corner of the user, the EAR calculated when the eye widely open is approximately 0.33 theoretically. In real-time video, the calculation might differ as there is real-life motion going on during the eye blinking detection.

The calculation for wide-open eyes:

$$EAR = \frac{\left||1cm|\right| + ||1cm||}{2\ ||3cm||}$$

$$EAR = \frac{2cm}{6cm}$$

$$EAR = 0.33$$

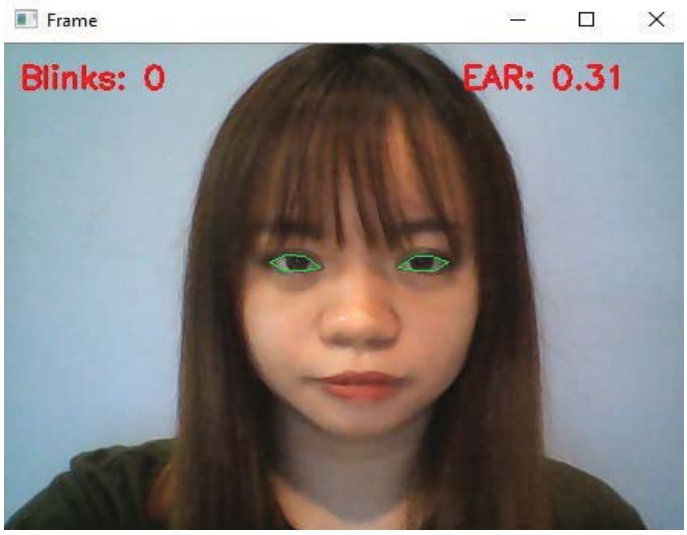


Fig. 7 shows the EAR results for the eyes that are wide open are approximately 0.31 which is a large and constant value, there is no decrease in value thus there is no changes in the count of eye blinks. The calculations are correct.

Fig. 8 shows the results of eye blinking detection and EAR value. There are no blinks detected yet thus the blink count is 0. The eyes are shut thus the EAR shows a smaller value. This part is where the design indicates that there is a blink ongoing. For example, based on the width and height of the eye corner of the user, the EAR calculated when the eye is tightly shut is approximately 0.067 theoretically.

The calculation for eyes tightly shut:

$$EAR = \frac{\left||0.2cm|\right| + ||0.2cm||}{2\ ||3cm||}$$

$$EAR = \frac{0.4cm}{6cm}$$

$$EAR = 0.067$$

The EAR results for the eyes that are tightly shut during the real-time video is 0.07 which is a small value, there is a large decrease in value thus there are will be changes on the count of eye blinks. The calculations are correct during real-time eye-blinking detection.

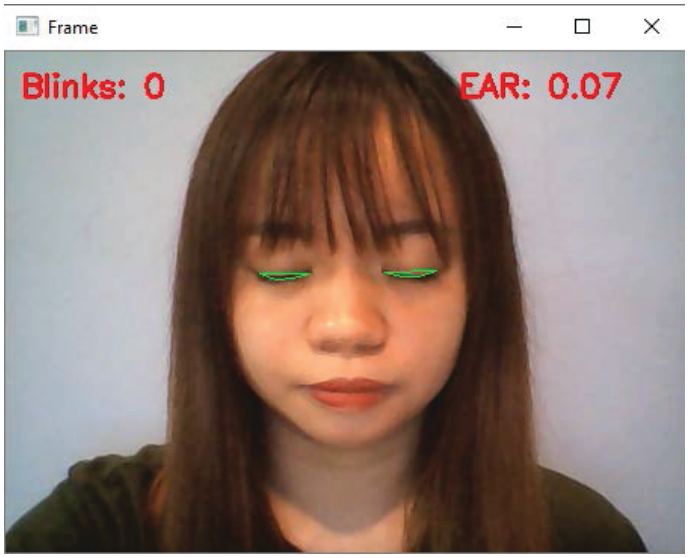


Fig. 8 shows the information of the eyes during the blink is going on, the EAR value at this point will be smaller and falls below the threshold level. Thus this marks that there is a blink going on.

Fig. 9 shows the results of eye blinking detection for the system. Once a blink is detected, the blink count will change to 1 because the EAR value had returned to the large and constant value which is 0.33 within a range for a wide-open eye.

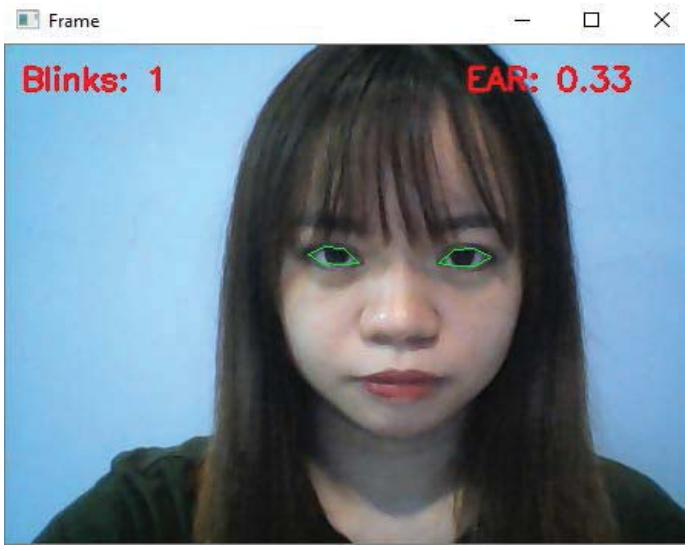


Fig. 9 shows the results of eye blinking detection for the system. Once a blink is detected, the blink count will change to 1. The real-time video for eye blinking detection is accurate. This will let the system proceed to the next step which is the automated login system.

Calculation for wide open eyes:

$$EAR = \frac{\left||1cm|\right| + ||1cm||}{2\ ||3cm||}$$

$$EAR = \frac{2cm}{6cm}$$

$$EAR = 0.33$$

3.3. Automated Login System

A script is designed to log in into the account of the owner on the university portal webpage. The script can be implemented using similar approach to any other webpage such as Facebook, Twitter or others. The username and password for the owner must be saved first inside the database to enable the auto-login system of the account.

Fig. 10 shows that the username and password of the owner of the account is automatically typed in by the automated test software inside Google Chrome webpage. The black color frame around the password section indicates that the password is typing into the blank space. Below the website link of the university portal also states that "Chrome is being controlled by automated test software."

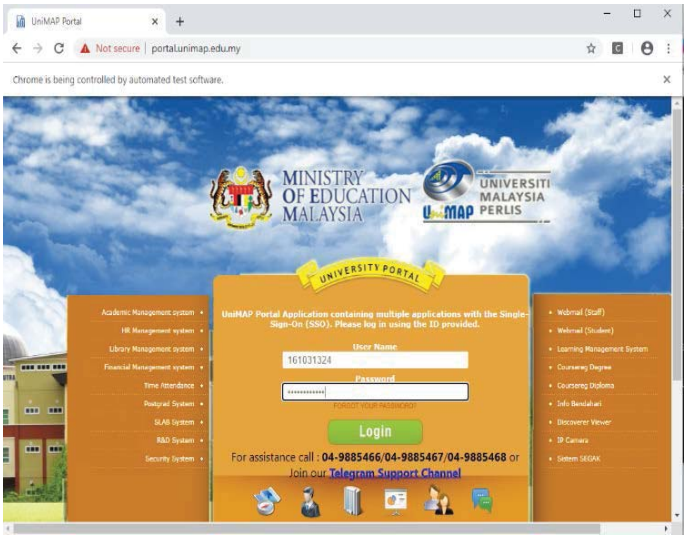


Fig. 10 indicates that the username and password of the owner is being inserted automatically.

Fig. 11 shows that the automated test software is controlling chrome by clicking the "login" button of the webpage after inserting all the username and password of the owner's database. The black frame around the login button means that the automated test software is entering the login button of the webpage, and the loading logo beside the website link is ongoing.

Fig. 11 shows that the login of the account is ongoing while Google Chrome is being controlled by automated test software.

Fig. 12 shows the successful login to the student's portal after using two-step verification. The process of identification starts by recognized the user's face and continued with eye blinking detection. If the user success login by using this approach, Google Chrome identified the website page as controlled via automated features.

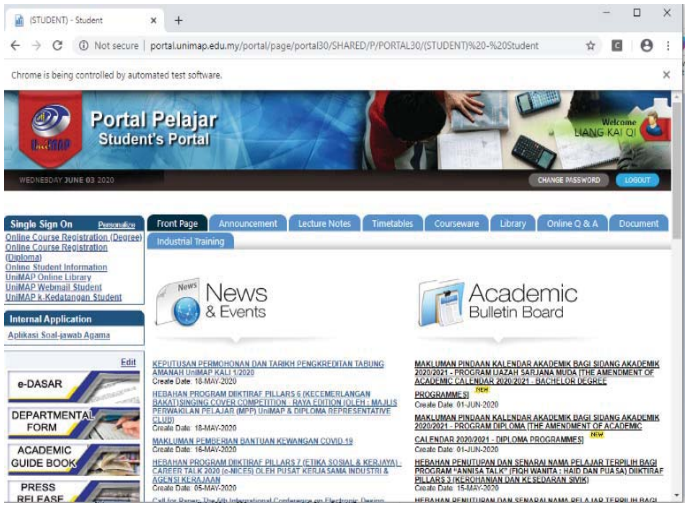


Fig. 12 shows the main webpage of the university portal after logging in. The description below the website link "Chrome is being controlled by automated test software" indicates that Google Chrome is controlled by the automated test program of the design.

4. Discussions

From the results obtained from real-time face recognition, it is found that the design works successfully after a few errors and trials had been done. The design is still can be improved for future development as there is still some improvement that can be done to enhance the performance as well as the security

level of the design. By designing the artificial intelligence security system, it can reduce a fraction of time for the user to login to their account of the webpage.

This security system concept not only can be applied onto accounts in websites, but it also can be implemented and improved for business applications such as payment verification for online business, logging in physical devices such as mobile phones, laptops, and more. It is a trend for security system designs to use the owner's face as the face ID for various account ownership but with higher security verification as blinking motion is needed throughout the process.

By using this face recognition with eye blinking security verification, the owner can increase the speed of logging into their account without typing any username and password and risking the fact that it can be hacked by hackers in the future. The owners only need to open the application system to confirm a payment using their camera on mobile phones. Facial biometrics are widely being practiced and used to more industries fields, such as design, construction, law enforcement, manufacturing, and healthcare. [11] Business can be done safer and easier by using this type of artificial technology system.

This can also help a lot of people with trouble keep forgetting their username or password details during logging in especially for the elders or the disabled people. For future development, users will be using this feature to get into their cars, houses, and other secure physical locations simply by just looking at the camera attached [12]. Facial recognition technologies are quickly growing and developing with new ideas such as 3-D modeling and others. [13-14] Face recognition with eye blinking security also could be important for a company or organization that handle sensitive data and needs double-layer authentication to control who enters their facilities. Artificial intelligence technology such as this project had become one of the most important technologies that can increase the lifestyle demand of humans. [15]

5. Conclusions

In this project, a two-step verification design that is the real-time face recognition with eye blinking to login an account is proposed. This verification technique aims to reduce the time for users to log in their accounts, increase the security awareness of account privacy, and also to increase convenience to users especially for elders and disabled people. During real-time face recognition, Open CV that is used for image processing is success and eye blinking motion detection is successful too. Besides that, the automated login can be conducted smoothly after both of the verification steps are done.

References

[1] S. Symanovich, "How does facial recognition work?", NortonLifeLock, 2020. [Online] Available: https://us.norton.com/internetsecurity-iot-how-facial-recognition-softwareworks.html
[2] W. Crumpler, "How Accurate are Facial Recognition Systems – and Why Does It Matter?", Center of Strategic & International Studies, 2020. [Online] Available: https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognitionsystems-%E2%80%93-and-why-does-it-matter
[3] D. Zeeuw. "Face Recognition", Electronic Frontliner Foundation, 2017. [Online] Available: https://www.eff.org/pages/face-recognition
[4] A.Belaweid, "Facial Emotion Recognition, Hands on guide!", Analytics Vidhya, 2020. [Online] Available: https://medium.com/analytics-vidhya/facial-emotion-recognition-hands-on-guide-8e23f3d0025f

[5] Adrian Rosebrock (2018), “OpenCV Face Recognition - PyImageSearch,” pyimagesearch.com [Online]. Available https://www.pyimagesearch.com/2018/09/24/opencv-face-recognition/.
[6] D. Taner, I. M. Bilasco, C. Djeraba, N. Ihaddadene, "Drowsy driver detection system using eye blink patterns." Machine and Web Intelligence (ICMWI), International Conference on. IEEE, 230-33, doi:10.1109/ICMWI.2010.5648121, 2010.
[7] T. Soukupova, J. Cech, "Eye Blink Detection Using Facial Landmarks." 21st Computer Vision Winter Workshop, Rimske Toplice, Slovenia, 2016.
[8] Pan, Gang, L. Sun, Z. Wu, "Eyeblink-based anti-spoofing in face recognition from a generic web camera.1-8, doi: 10.1109/ICCV.2007.4409068, 2007.
[9] Adrian Rosebrock (2017), “Eye blink detection with OpenCV, Python, and dlib - PyImageSearch,” pyimagesearch.com,. [Online]. Available: https://www.pyimagesearch.com/2017/04/24/eye-blink-detection-opencv-python-dlib/.
[10] M. Brahimi, “How to Build a Simple Auto-Login Bot with Python and Selenium”, Hongkiat.com (HKDC), 2018. [Online] Available: https://www.hongkiat.com/blog/automatecreate-login-bot-python-selenium/
[11] L. Cox, (2017) “5 Applications of Facial Recognition Technology - Disruption Hub,” Disruption,. [Online]. Available: https://disruptionhub.com/5-applications-facial-recognition-technology/.
[12] A. Kahnin (17th May 2018), “Modern Face Recognition Systems | Security Industry Association,” Sia Technology Insight,. [Online]. Available: https://www.securityindustry.org/2018/05/17/modern-face-recognition-systems/.
[13] B. Knyazev, R. Shvetsov, N. Efremova, A. Kuharenko, “Leveraging Large Face Recognition Data for Emotion Classification”, 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, pp. 692-696, 2017.
[14] R. He, J. Cao, L. Song, Z. Sun and T. Tan, "Adversarial Cross-Spectral Face Completion for NIR-VIS Face Recognition," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 5, pp. 1025-1037, 2020.
[15] C. Gahnberg, R. Polk “Artificial Intelligence and Machine Learning: Policy Paper”, Internet Society, 2017. [Online] Available: https://www.internetsociety.org/wpcontent/uploads/2017/08/ISOC-AI-Policy-Paper_2017-04-27_0.pdf