International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Gaze Gesture Authentication System Against Shoulder Surfing Attacks

Manish Pillai[1], Srivenkatesh Nair [2], Sujith Kurup[3], Abhinav Menon[4], and Prof. K.S. Charumathi[5]

[1]BE Student, Department of Computer Engineering, Pillai College of Engineering, Navi Mumbai - 410206
[2]BE Student, Department of Computer Engineering, Pillai College of Engineering, Navi Mumbai - 410206
[3]BE Student, Department of Computer Engineering, Pillai College of Engineering, Navi Mumbai - 410206
[4]BE Student, Department of Computer Engineering, Pillai College of Engineering, Navi Mumbai - 410206
[5]Assistant Professor, Department of Computer Engineering, Pillai College of Engineering, Navi Mumbai - 410206

Abstract - Shoulder surfing is the term used to describe one person observing another person's computer or mobile device screen and keyboard to obtain sensitive information. Direct observation can be done by simply looking over someone's shoulder – hence shoulder surfing – or using binoculars, video cameras, and other optical devices. Shoulder surfing usually has the goal of viewing and stealing sensitive information such as username and password combinations that can be used to enter a user's account later. Credit card numbers, PIN, and sensitive personal information used in response to security questions are also targeted. So, the proposed Two-factor authentication would secure the system from the Shoulder Surfing Attack which is disparate from the traditional existing system where username and password are required for authentication. In the proposed system, the first phase is username & password validation just like a login page. The information for authentication is provided by the user while registering to the page. In the next phase, Gaze Gesture Authentication is used through Real time eye tracking using OpenCV and Dlib. Through multiple evaluations, we discuss how the authentication accuracy varies with respect to transition speed of numbers and user's blink.

Keywords: Shoulder Surfing, Gaze Gesture, Authentication, Security, Eye Tracking, Patterns.

1. INTRODUCTION

Shoulder Surfing Attacks have become a widespread problem in today's world and there are very few systems available that are used to prevent these attacks. There has also been an increase in the development of interactions between humans and computers. This is where Gaze Gesture plays an important role. Gaze gestures provide an effective hands-free modality for human–computer interaction. The gaze gestures are recognized based on directions of gazes and extract the gaze gestures based on the same. Such a system reduces the chances of Shoulder Surfing Attacks as no physical interactions take place between the user and the computer for the attacker to observe or record.

2. LITERATURE SURVEY

A. PIN entry based on Gaze Technique:

PIN requires users to put the input manually, which could lead to loss of sensitive information due to shoulder surfing attacks. In order to prevent this, Gaze based authentication (tracking eye location and eye movement) is used which means entering the PIN without entering the password manually which is more secure.

B. Eye Detection Algorithm:

The user has to stare at a pin for a few seconds and then stare at the next. Tracking algorithm first captures the face and then the position of the eyes. The coordinate system conversion is accomplished to standardize the coordinates of the reported eye location, to allow capturing the eye at various angles based on the tilt of the head. For PIN identification, the eye center coordinates (horizontal and vertical) in the spreadsheet are first plotted on a 2D spreadsheet. Then the data points are grouped using clustering.

C. Eye gaze or eye tracking:

It is characterized as the methodology of the recognition of the eye position through video record outlines used for the assurance of the situation of the look. The entire procedure can be partitioned to four phases, for example, face Identification, eye recognition, understudy location and eye gaze. This framework uses a USB or inherent webcam for catching and distinguishing the developments of the client's face.

D. Scan-path Matching Algorithm:

The System matches the user's scan-path against a circle's traversed path through the "Template Matching" algorithm, where we compute the root-mean-square distance of the candidate path (user's scan-path) from all the template paths (circles' traversed paths). The template path of a circle that is at the least root-mean-square distance from the candidate path is chosen as the circle (color) followed by the user. Our template matching algorithm is based on $1, but we perform only sampling, and calculate the average distance between the two paths.

E. Directional Based Graphical Authentication:

This method used by Noor Ashitah Abu Othman, Muhammad Akmal Abdul Rahman, Anis Shobirin Abdullah Sani, Fakariah Hani Mohd Ali is a modified part of the Passface scheme with addition of direction image such as it used animal faces instead of human faces since it is more distinguishable by people in order to conceal the password.

3. PROPOSED SYSTEM

Selecting password using eye movement:
Controlling the computer mouse with the eyes demands a quick and effective algorithm, which has enabled us to reduce the tool's operating time to the bare minimum by splitting the operation into a few steps and using a tracking algorithm in order to avoid unnecessary calculations.

3.1 System Architecture

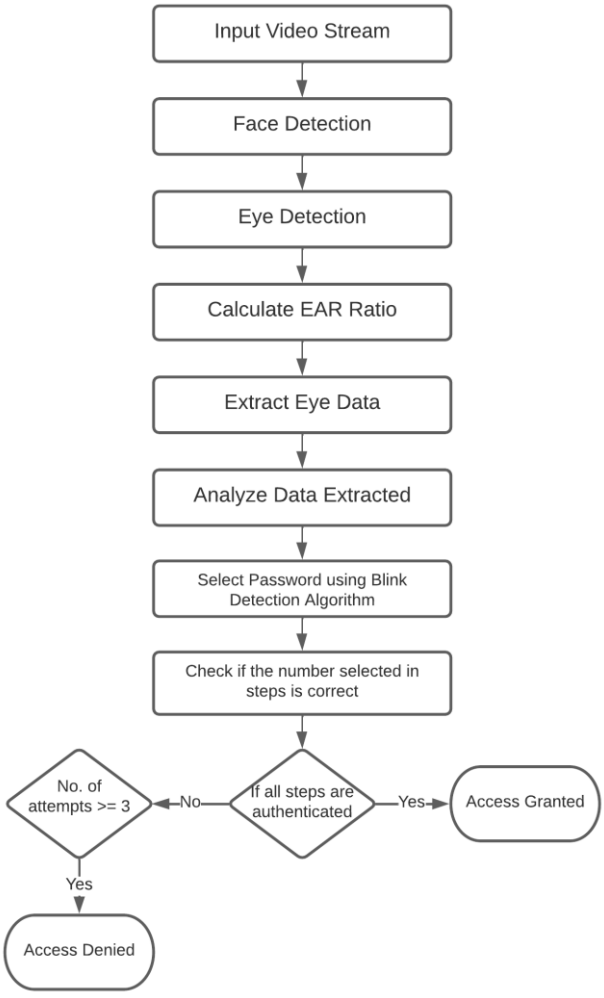

Fig.1: System Architecture

The system architecture is given in Fig. 1. Each block is described in the given section.

A. Input Block Description

The face is detected at the first using a Haar Cascade Based Algorithm. It represents the faces efficiently using Facial Landmarks. The algorithm uses a facial training set to understand where certain points exist on facial structures. The program then plots the same points on regions of interest in other images, if they exist. Priors are used by the software to determine the likely distance between critical spots. Its outposts a 68-point plot of the given image or real time face.

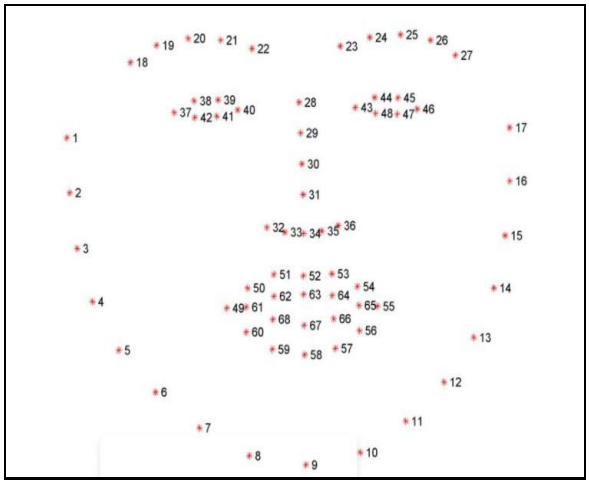

Fig.2: Facial Landmarks

B. Eye Tracking Block

For eye blinking we need to pay attention to points 37-46, the points that describe the eyes. Then we use the Eye Aspect Ratio for further procedure, the eye aspect ratio can be defined as "A constant value when the eye is open, but rapidly falls while the eye is closed, to 0." If the Eye Aspect Ratio goes below a specific level, the computer can tell if an user's eyes are closed.

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

Fig.3: Eye Aspect Ratio

C. Authentication Block

The moment the user blink's first time for a particular step, the password is selected.
Once the step is completed, the system compares the selected password with the password the user had given at time of registration. If the password is correct, the process continues till the final step. Else, the user would be given 2 attempts to retry, that step failing on which the user has to retry from start. The restriction is 3 attempts for the entire retry.

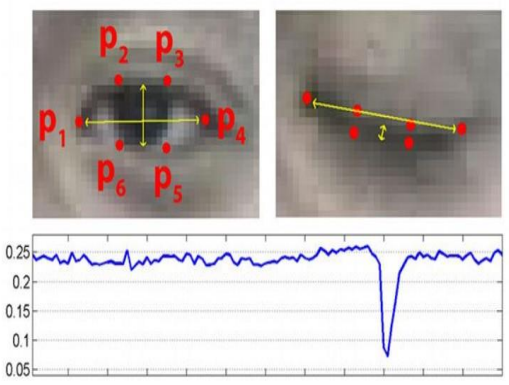

Fig.4: Eye Landmarks

D. Output Block Description

After all the steps are authenticated, the user is given access to the system.

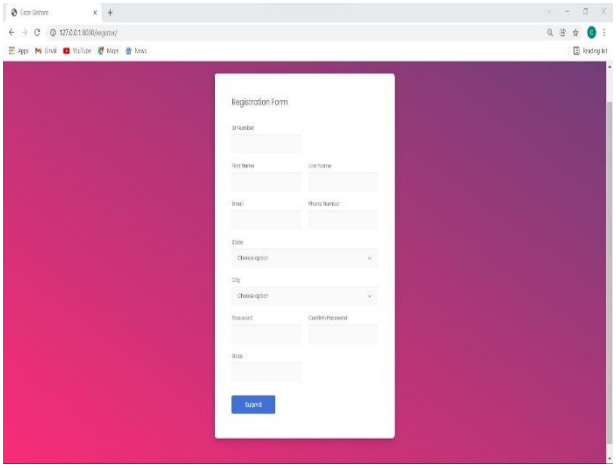

Fig.5: Registration Page

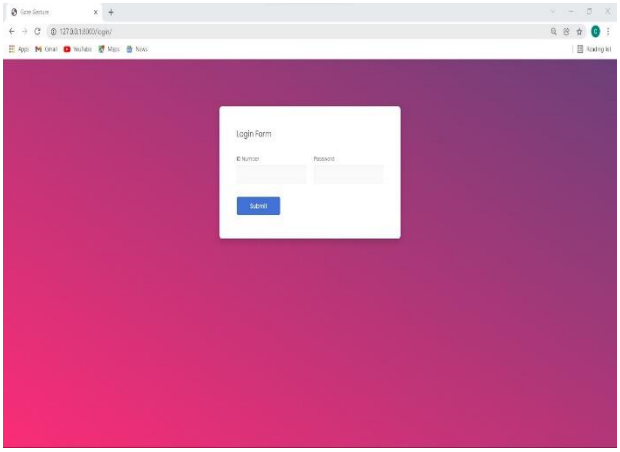

Fig.6: Login Page

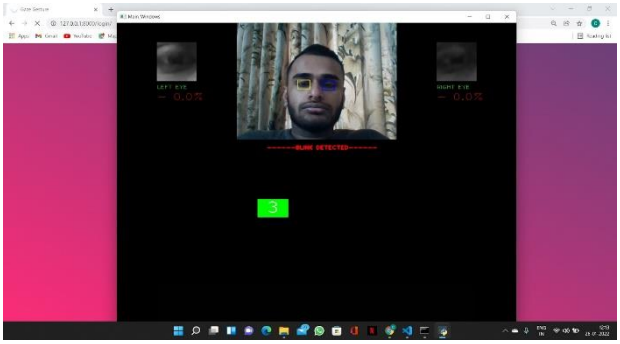

Fig.7: Blink Detection

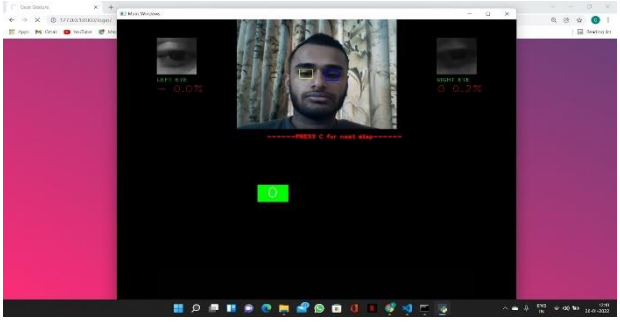

Fig.8: Correct Password Entry

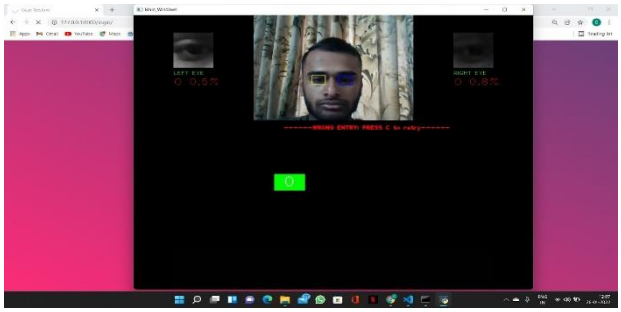

Fig.9: Wrong Password Entry

4. CONCLUSION

This paper proposed a Gaze Gesture based Authentication System for prevention against Shoulder-Surfing Attacks. The proposed system uses a Blink Detection Technique which conceals the user's password from the attacker. The implementation process was carried out under observation to find out the percentage of successful authentication, number of attempts required to authenticate and the time taken for the entire process. The results displayed that the proposed algorithm provided a high authentication success rate. Majority of the participants were able to authenticate in 2 to 3 attempts without any issues making the system highly accurate. On an average, it takes around 3 - 4 minutes for the entire authentication process. The results show that the proposed method efficiently prevents shoulder-surfing attacks.

Future Scope:

In the future, further research for implementing a face detection feature to validate the user will be our main focus in order to increase security. Moreover, this system can be converted into a package, making the project available for various domains such as ATM machines or unlocking desktops and so on.

ACKNOWLEDGEMENT

It is our honour to thank our supervisor, Prof. K.S. Charumathi, for her valuable contributions, capable leadership, encouragement, wholehearted cooperation, and constructive criticism during the course of this project. Dr. Sharvari Govilkar, our Department Head, and Dr. Sandeep M. Joshi, our Principal, deserve our heartfelt gratitude for encouraging and permitting us to share this work.

REFERENCES

[1] Por, L.Y.; Adebimpe, L.A.; Idris, M.Y.I.; Khaw, C.S.; Ku, C.S. LocaPass: A Graphical Password Method to Prevent Shoulder-Surfing. Symmetry 2019,11, 1252. Url: https://doi.org/10.3390/sym11101252

[2] V. Rajanna, A. H. Malla, R. A. Bhagat and T. Hammond, "DyGazePass: A gaze gesture-based dynamic authentication system to counter shoulder surfing and video analysis attacks," 2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA), 2018, pp. 1-8, doi: 10.1109/ISBA.2018.8311458.

[3] H. Sun, S. Chen, J. Yeh and C. Cheng, "A Shoulder Surfing Resistant Graphical Authentication System" in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 02, pp. 180-193, 2018. doi: 10.1109/TDSC.2016.2539942
[4] Mehrubeoglu, Mehrube, and Vuong Nguyen. "Real-time eye tracking for password authentication." 2018 IEEE international conference on consumer electronics (ICCE). IEEE, 2018.
[5] Rahman, TR Muhibur, K. Neha, and M. Reshma. "REAL TIME EYE TRACKING FOR PASSWORD AUTHENTICATION." International Journal of Advanced Research in Computer Science 11.3 (2020).