IJRESM
International Journal of Research in Engineering, Science and Management
Volume 4, Issue 7, July 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Real Time Eye Blink Password Authentication

Aravinda Thejas Chandra[1], G. Sneha[2], Srushti Anand[3*], C. Yashaswini[4]
[1]*Associate professor, Department of Information Science and Engineering, S. J. C. Institute of Technology, Chikkaballapur, India*
[2,3,4]*Student, Department of Information Science and Engineering, S. J. C. Institute of Technology, Chikkaballapur, India*

***Abstract*: Personal identity numbers are extensively used for consumer authentication and safety. Password verification the use of PINs calls for customers to go into a bodily PIN, which may be liable to password breakage or hacking through shoulder surfing or thermal tracking. PIN authentication with hands-off eye blinks PIN access strategies, on the opposite hand, leaves no bodily footprints in the back of and consequently gives an extra stable password access option. Eye blinks primarily based totally authentication refers to locating the eye blinks throughout sequential image frames, and generating the PIN. This task affords a real-time software we integrate eye blink primarily based PIN entry, and face detection and OTP (One Time Password) to keep away from shoulder surfing and thermal tracking attacks.**

***Keywords*: Shoulder surfing, Thermal tracking, Adaboost training, Cascading classifier.**

1. Introduction

One of the safety necessities for well-known terminal authentication systems is to be easy, speedy and secure as human beings face authentication mechanisms each day and have to authenticate themselves use of traditional know- how primarily based totally tactics like passwords. But those strategies aren't safe due to the fact they may be regarded via way of means of malicious observers who use surveillance strategies such as shoulder-surfing to seize consumer authentication statistics. Also there are security issues because of terrible interactions among systems and customers. As a result, the researchers proposed a 3 layered security framework to stable PIN numbers, in which customers can input the password by blinking the eye at the perfect symbols in an appropriate order and consequently the consumer is invulnerable to shoulder surfing. Eye blinking is an herbal interplay technique and security systems based on eye blink tracking offer a promising way to the system security and usability. The aim of this paper is to check techniques or solutions to managing eye blink in security systems.

2. Objectives

- To input and pick out eye blink primarily based totally PINs the use of a clever smart camera through real-time eye detection and tracking.
- To keep away from shoulder surfing attacks, Flawless identification authentication.

3. Algorithm Specification

A. *HAAR Cascade Face Detection*

Haar Cascade is a machine learning object detection algorithm used to identify objects in an image or video and primarily based totally at the idea of capabilities proposed via way of means of Paul Viola and Michael Jones of their paper "Rapid Object Detection using a Boosted Cascade of Simple Features" in 2001.It is a machine learning based approach in which a cascade feature is trained from a whole lot of positive and negative images. It is then used to detect objects in other images.

The algorithm has four stages:

1. Haar Feature Selection
2. Creating Integral Images
3. Adaboost Training
4. Cascading Classifiers

B. *Local Binary Pattern Histogram*

Local Binary Patterns Histogram algorithm was proposed in 2006. It is based on local binary operator. It is extensively utilized in facial recognition because of its computational simplicity and discriminative power.

The steps involved to achieve this are:

1. creating dataset
2. face acquisition
3. feature extraction
4. classification

4. Implementation

A. *Modules*

1) *Capturing the face*

Since the Face is symmetric, we use a symmetry-based method. We observed that it's miles enough to apply a sample version, that' s a gray scale. The symmetry see is calculated after which calculated throughout the pixel columns in the reduced image. If the image is represented as I(x, y) within side the decreased picture. If the picture is represented as I(x,y) then the symmetry value for a pixel-column is given via way of

*Corresponding author: srushtianand@gmail.com means of S(x) = ∑∑ [abs I ((x, y-w)-(x, y+w))]. S(x) is computed for X € [k, size-k] where k is the maximum distance from the pixel-column that symmetry is measured, and x size is the width of the image. The x corresponding to the lowest value of S(x) is the center of the face.

2) Tracking of the eyes

We track the eye by looking for the darkest pixel in the predicted region. In order to recover from tracking errors, we make sure that none of the geometrical constraints are violated. If they are, we re-localize the eyes in the next frame. To find the best match for the eye template, we initially center it at the darkest pixel, and then perform a gradient descent in order to find a local minimum.

3) Authentication of user

We are collecting the generated PIN and checking with the system databases if user id and PIN matches, System will send OTP to the user's mobile number if user enters the correct OTP system will authenticate the user.

We are going to propose the three-layer security scheme to avoid the shoulder surfing and thermal tracking attacks. Our system contains the three layers which are 1. Face reorganization, 2. Eye-blink verification. and 3. OTP by combining all this layers we are going to implement our secure framework to avoid shoulder surfing and thermal tracking attacks. In our frame works there is no physical entry of password so we are completely avoiding the shoulder surfing and thermal tracking attacks. For the first layer security we are using Deep Learning algorithm, for the second layer we are using OpenCV.

5. Design

A. Flowchart

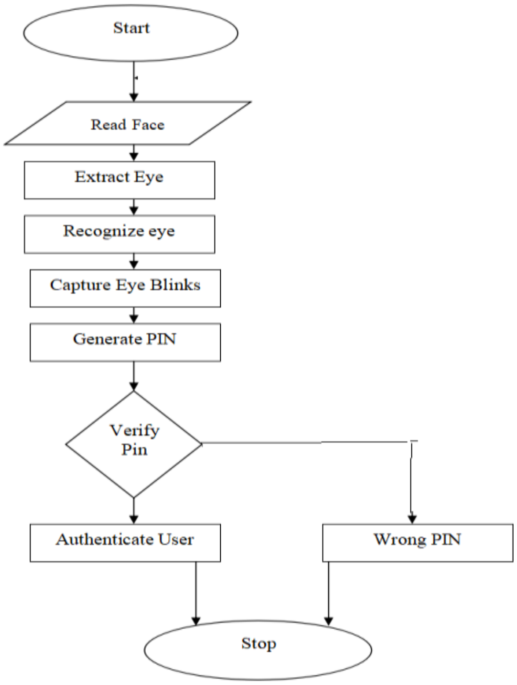

Fig. 1. Flow chart

B. Data flow diagram

Level 0

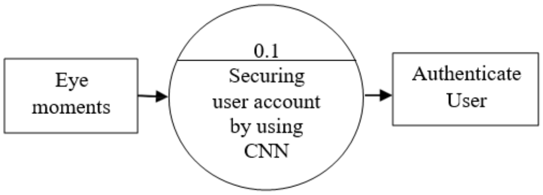

Fig. 2. Level 0 of data flow diagram

Level 1

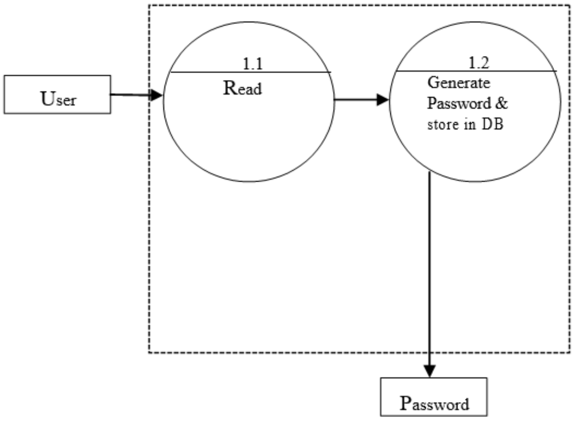

Fig. 3. Level 1 of data flow diagram

Level 2

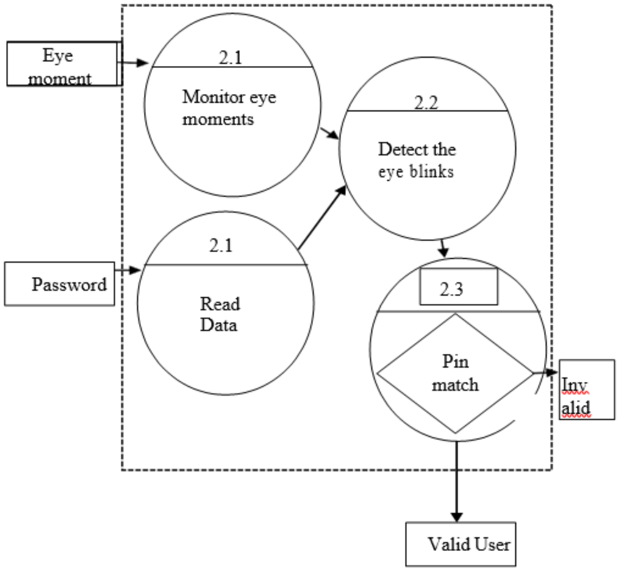

Fig. 4. Level 2 of data flow diagram

6. Result

The large volume of data was conducted in order to access system accuracy and all the cases were successful. The password can be authenticated without the manual entry of the PIN. This method avoids Shoulder-Surfing, Thermal Tracking which can be a threat to the user. This is the safe method to authenticate the PIN. This method accuracy is high, everyone can use easily, little time consuming, cost efficient and easy to implement. This clearly show that password authentication using blinking method is more efficient than the other method. The numbers of cases were experimented on this model using the conditions: PASSWORD MATCH and PASSWORD NOT MATCH any some more in which all the cases were 100% accurate. This is the new method that has not implemented earlier and this method is more secure than the physical entry of PIN which causes threats like shoulder-surfing, thermal tracking etc.

7. Conclusion

A smart-camera based eye-tracking system has been incorporated into a new application for gaze-based PIN identification. The system has been successfully tested with a nine-digit keypad, and can be extended to character and digit combination password entry. Stray data points in the scatter plots are generally associated with transitional movement of the eyes between digits. In addition, screen size affects the precision within the clusters, and must be calibrated for each screen and keypad. The stability of the consumer's gaze will affect the accuracy of the detected pins, and must be accounted for. Currently, the PIN identification is accomplished after real-time eye-tracking and eye center computations and recording are completed.

References

[1] R. Revathy and R. Bama, "Advanced Safe PIN-Entry Against Human Shoulder-Surfing," IOSR Journal of Computer Engineering, vol. 17, issue 4, ver. II, pp. 9-15, July-Aug. 2015.

[2] J. Weaver, K. Mock and B. Hoanca, "Gaze-Based Password Authentication through Automatic Clustering of Gaze Points," Proc. 2011 IEEE Conf. on Systems, Man and Cybernetics, Oct. 2011.

[3] ATM Fraud, ATM Black Box Attacks Spread Across Europe, European ATM Security Team (E.A.S.T.), April 2017. https://www.europeanatm-security.eu/tag/atmfraud/

[4] K. Mowery, S. Meiklejohn and S. Savage, "Heat of the Moment: Characterizing the Efficacy of Thermal Camera Based Attacks," WOOT'11, pp. 1-8, August 2011.

[5] M. Mehrübeoglu, H. T. Bui and L. McLauchlan, "Real-time iris tracking with a smart camera," Proc. SPIE 7871, 787104, 2011.

[6] M. Mehrubeoglu, L. M. Pham, H. T. Le, M. Ramchander, and D. Ryu, "Real-time eye tracking using a smart camera," Proc. 2011 IEEE Applied Imagery Pattern Recognition Workshop (AIPR '11), pp. 1-7, 2011.

[7] M. Mehrubeoglu, E. Ortlieb, L. McLauchlan, L. M. Pham, "Capturing reading patterns through a real-time smart camera iris tracking system," Proc. SPIE, vol. 8437, 2012.

[8] Smart Cameras for Embedded Machine Vision, (product information) National Instruments.