ISSN No. 0976-5697

Volume 11, Special Issue I, May 2020

International Journal of Advanced Research in Computer Science

CONFERENCE PAPER

Available Online at www.ijarcs.info

REAL TIME EYE-TRACKING FOR PASSWORD AUTHENTICATION

Tasmiya Mairaj
UG Student, School of C & IT,
REVA University
Bangalore, India
tassu03031998@gmail.com

Vrinda Gopakumar
UG Student, School of C & IT,
REVA University
Bangalore, India
Vrindagopakumar21@gmail.com

Zaveriya Roshan
UG Student, School of C & IT,
REVA University
Bangalore, India
rzoya24399@gmail.com

Priyanka Bharti
Professor, School of C & IT,
REVA University
Bangalore, India
priyankabharti@reva.edu.in

Abstract- Real-time eye tracking is vital for hand free blink-based password entry. PIN's (password authentication numbers) are extensively used for security and authentication. PINs are largely used for safety reasons. Password authentication works when a user enters the password using his hands, which might lead to cracking the password through techniques like shoulder surfing or thermal tracking. Authentications with eye blink techniques, does not leave any traces behind as there is no movement or contact with the keyboard during password entry and thus provides a safe environment. Eye tracking helps in locating the image frames sequentially and tracks the center of the eye. This project introduces an application in which we are combining eye blink tracking PIN entry, face detection/recognition and OTP (One Time Password) to avoid shoulder surfing and thermal tracking attacks.

Keywords- User authentication, OTP(one time password), CNN, Eye blink PIN entry, Face detection

.

I. INTRODUCTION

One of the safety needs for general terminal authentication systems is to be simple, quick and secure as individuals face authentication mechanisms daily and should demonstrate themselves victimization standard knowledge-based approaches like passwords. however these techniques don't seem to be safe as a result of their viewed by malicious observers World Health Organization use police work techniques like shoulder-surfing (observation user whereas typewriting the word through the keyboard) to capture user authentication knowledge. Conjointly there square measure security issues because of poor interactions between systems and users. As a result, the researchers projected a 3 bedded security framework to secure PIN numbers, wherever users will enter the word by blinking the attention at the {appropriate} symbols within the appropriate order and therefore the user is inviolable to shoulder aquatics. Eye blinking could be a natural interaction technique and security systems supported blink pursuit give a promising answer to the system security and value. The aim of this paper is to review techniques or solutions to handling eye blink in security system.

II. LITERATURE SURVEY:

Many methods had been used till date for password authentication, which has resulted to password thefts.

1.Title: Advanced Secure PIN-Entry avoiding Shoulder-Surfing

Abstract: When users place their passwords in a common area, they might be at risk of attacker stealing their password. The PIN is recognized by closing by the adversary, more effectually in a busy place. A new technique has been accepted to cope up with this problem that is cryptography preventing techniques

2.Title: CHARACTERIZATION OF THE EFFICIENCY OF THERMAL CAMERA ATTACKS.

Author: Keatonn Mower, Sarahh Meiklejon, Stifan Savag

Abstract: during this paper, we inspect the probable of employing a thermal camera to recuperate code entered on the keyboard during a sort of scenario. This attack has the benefits over employing a standard camera that the codes don't need to be captured while they're being put and may instead be recovered for a brief period afterwards. To urge the widely view of how effective such an attack could be, we consider variety of variables: the fabric of the keypad, the user entering the code, the space from the camera to the keypad.

3.Title: GAZE-BASED PASSWORD AUTHENTICATION THROUGH AUTOMATIC CLUSTERING OF GAZE POINTS AUTHOR: Justin Weaver, Kenrick Mock, Bogdan Hoanca.

Abstract: Analysts have suggests systems during which user uses a fixed eye tracker to enter passwords by truly watching the right cipher on the pc so as. Instead, in Eye cavity details are mechanically gathered to work out the user's cipher; this proceeding has the advantage of allowing users to validate at their likely speed, instead by a hard and fast stay time.

III. OBJECTIVES:

- To resist the shoulder surfing attacks in the user authentication system.
- To resist the thermal tracking attacks in keyboards.
- To provide three layered security for user authentication.

IV. METHODOLOGY:

Facial Recognition using CNN:

Facial expressions involve extensive and diverse areas in the brain because the face interpretations are very complicated. Our brain can process the whole face and it also can recognize an individual even by the half of the face. The brain differentiates the interior averaged pattern with the resulting picture and finds characteristic differences. Steps related to Facial recognition:

- You would like to appear at the image and realize all the faces are present.
- It's necessary to focus on every face and confirm that, despite the unnatural turn of the face or poor lighting, it's an identical person.
- It's necessary to spotlight the unique characteristics of the face, which can be used to distinguish it from one person to another.
- It's important to compare the characteristics of other people with the unique characteristics of the face, so that the name of the person can be identified.

Working Of Facial Recognition System:

Initially, the face identification method must locate a face within the picture and emphasize the areas. There are sort of algorithm for this software. To make decision on the choices of contours within the picture and their contrast with the contour of faces. Similarity of proportions and complexion, the choice of symmetries using neural networks. The foremost efficient one which may be utilized in real time is the Viola-Jones method. With that, the system can recognizes the faces even when it rotates at 30 degrees.

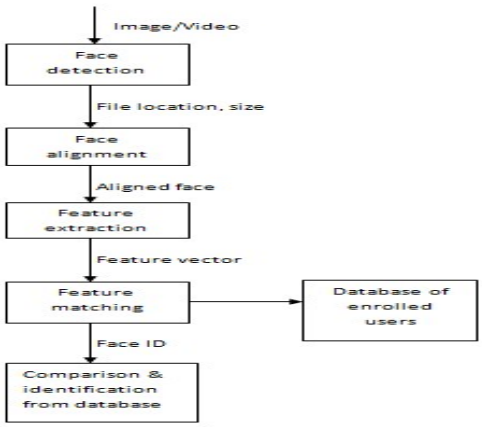

Fig.1: Face recognition processing flow.

However, the system is developed in such a way that it compares the results with the acquired data by a correct acquisition that detects the image of the face. Thereby, helping it to track and select the optimum angle and image is processed accordingly. Image is processed based on the principle of motion vector algorithm or correlation algorithm.

With this certainty, system chooses and recognise it's images for comparing the existing base. This is internally connected with this base and the program finds the orientation position through people's face which develops the technical feature individually.

Those points are awarded based on its methods carried out. Finally, measurement is carried out for face recognition, that can be found through a set of string such as the distance between the eyes , the measurement of the nostrils , the length of the nose , the elevation and figure of the cheekbones , the distance across of the chin , the stature of the forehead and other certainty. Therefore, data

is then compared with the available parameters on the database and hereby person's image is identified.

Eye Blink Password Generation:

This is the second layer of authentication that we are displaying by digital keyboard on the screen. On the digital numeric keyboard, a cursor will keep moving as the person blinks, therefore the eye system will generate the pin number based on the sequence collected by the number of blinks. To monitor the eye movements, we are using web camera. Based on the conception that we are going to build by detecting eye blinks using OpenCV, a PC image application can be developed which is capable of detecting and counting blinks into films using facial landmark and OpenCV. We'll be computing a metric called the eye feature proportion, to build our blink detector. A distinct traditional image for computing blinks through processing methods typically involves the following:

- Localization of the eye.
- To find the "whites" of the eye using thresholding.
- To indicate a blink, a "white" area of the eye disappears for duration of time.
- An effective solution to the eye aspect ratio which typically engages a very easy result depending on the share between facial landmarks of the eyes.

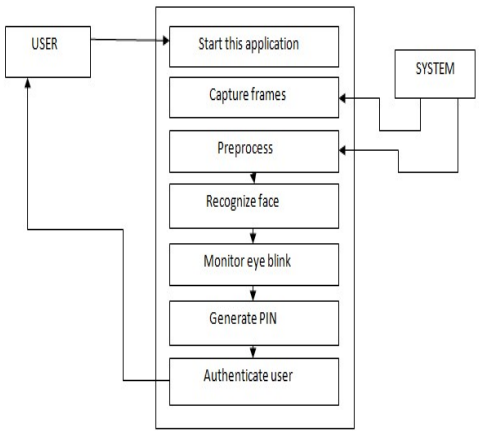

Fig.2: Workflow of the project

OTP generation and verification: This is the third level of authentication where OTP means one time password. To generate the OTP we are using random numbers and that numbers are send to users email/phone number. By using this method we can verify and secure the account.

V. Modules Identified:

- Locating the Face
- Tracking eye coordinates
- CNN Model

Locating the Face: Each pixel-column during a reduced image computes a symmetry-value. For image I(x, y) the symmetry worth is given as $S(x) = \sum\sum [abs\ I\ ((x, y-w)-(x, y+w))]$. Here S(x) is evaluated for X € [k, size-k], where k is that the space between the pixel -columns in a picture, and x size is that the image breadth.

Tracking eye coordinates: we tend to follow the eye by searching for the darkest component within the expected area. So as to live through trailing error, we check that that none of the statistical limit area unit desecrated. If they are, we re-localize the eyes within the next framework.

CNN Model:

This step is the most vital part of the whole method as we style the CNN through that we are going to pass our options to coach the model and eventually see its mistreatment to the check options. We've used a mix of many totally different functions to construct CNN.

VI. RESULTS AND DISCUSSIONS

We have implemented the web based application which it contains the three layer security to provide the security to avoid the illegal access of our accounts.

.

Below are some of the screenshot:

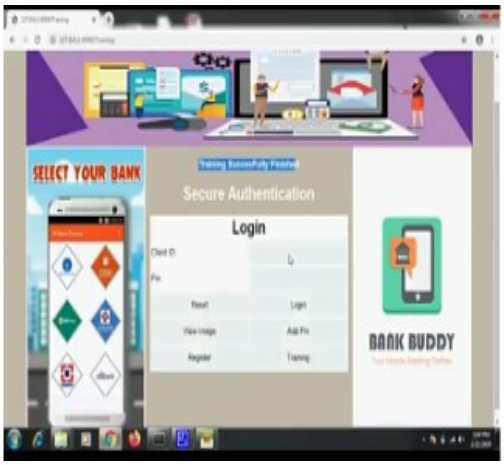

Fig 4: Login page for the user.

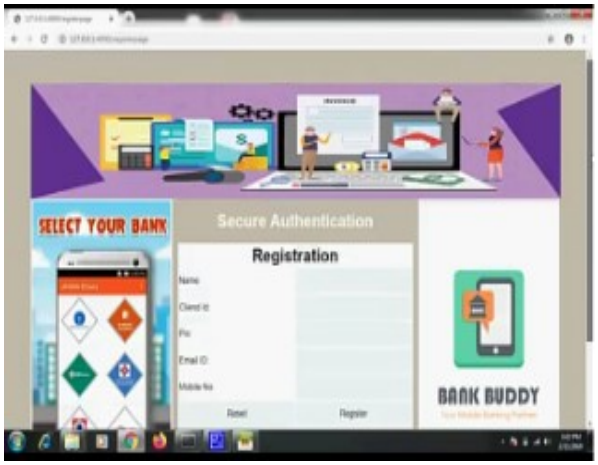

Fig. 5: Registration page for safe authentication.

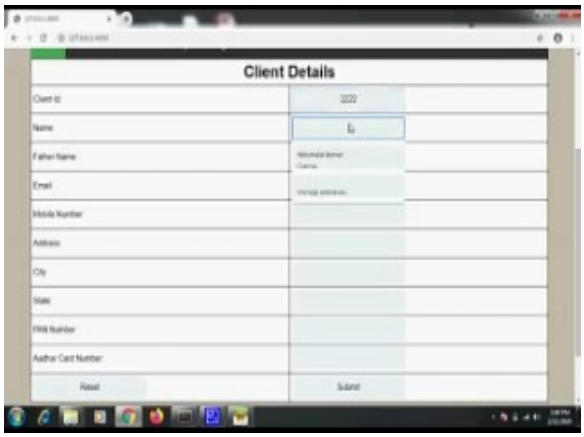

Fig.6: Client details are recorded for more convenient and secure system.

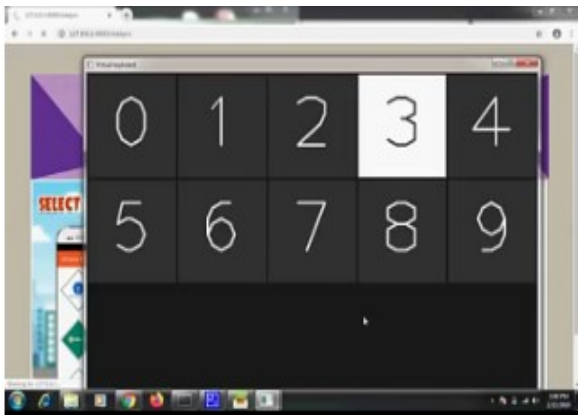

Fig. 7: Visual keyboard for password entry.

Fig.8: client details entered are displayed on the screen.

VII. CONCLUSION

The new application called eye blink based PIN identification has been incorporated using a small camera based system. This system has nine-digital keypad which has been tested successfully, and the system can also continue with combination password entry. The stability of the user eye blink will affect the correctness of the detected PIN and must be accounted for. Presently, the pin identification is accomplished after eye center identification and real time blinks and recording are computed.

VIII. FUTURE SCOPE:

While our project provides promising results, it can still be upgraded in the coming future. We can strengthen a password by withdrawing additional bits from the gaze path that the user follows while entering the password. For more secure authentication in the near future we can add a person's thumb impression for accessing the account. Even different gaze patterns to be accepted by the system so that the attacker cannot mimic the user's gaze path.

IX. REFERENCES:

[1] Revath and Bamai introduced "Advanced Safe PIN-Entry Against Human Shoulder-Surfing," in IOSR

[2] J. Wever, Mock and B. Honca implemented "Gaze-Based Password Authentication through Clustering of Gaze Points."

[3]"ATM Fraud, ATM Black Box Attacks Spread across Europe", (E.A.S.T.), posted 11 Apr-17.

[4] K. Mowry, S. Meklejohn and Savag researched on "Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks," WOOT '11, Aug-11.

[5]. Mohamed, Florian, Mariam, Emanuel, Regina and Andreas "Gaze-Touch Pass Scheme", March 2016.

[6]. Anjit George, Aurobind Routray "Real time Eye Direction Classification Using Convolutional Neural Network", June2016.

[7]. Puja sorat, Prof. Chajed Paper on "Eye Tracking Methods and Techniques", in the IRJET.

[8] M. Mehrubeglu, E. Ortlib, L. McLauclan, M. Pham, "Capturing reading patterns through a real-time smart camera iris tracking system," Proc. SPIE.