iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44434

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

EYE Blinking for Password Authentication

Dr. Sharavana Kumar R[1], Yashaswini S[2], Deepakraj N[3], Rakshitha E S[4], Chandana V[5]
[1, 2, 3, 4, 5]*BE Students, Department of Computer Science and Engineering Asst. Professor, Department of Computer Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India*

Abstract: Personal identification numbers area unit used for user authentication and security. word verification exploitation PINs requires users to enter a physical PIN, which may be vulnerable to word breakage or hacking via shoulder water sport or thermal chase. PIN authentication with eye blinks entry techniques, doesn't leave any quite physical footprints behind and therefore provide a safer word entry possibility. This project presents a time period application to avoid. The personal identification numbers (PINS) is a common user authentication method for many applications, such as money transaction is online banking application and automatic teller machine(ATMs).unlocking personal devices ,event centers, shopping malls, Medical centers, schools/collages and opening Doors.

I. INTRODUCTION

Today, the net has entered into our daily life and all the services are stirred on-line. on the far side reading the news, trying to find info, and different threat free task, we have conjointly become acquainted with different risk-related work, such as paying victimization credit cards, checking/composing emails, on-line banking, and so on. whereas we have a tendency to appreciate its benefits, we have a tendency to square measure putting ourselvesin danger. Eye trailing is that the method of police investigation the attention location across video frame. The motion of the attention relative to the pinnacle may also be additional interest. Eye trailing is vital for development and analysis areas like visual systems, psychological analysis, scientific discipline and products style. An eye trailing system is associate integration of agroup of devices and associated programs for mensuration eye positions and movement, and correlating the results to a similar eye across images non inheritable consecutive over time.

II. LITERATURE REVIEW

A. Title: Advanced Safe PIN-Entry Against Human Shoulder-Surfing

Author: Ms. R Revathy, Mrs..Bama2

When users insert their passwords in a common area, they might be at risk of aggressor stealing their password. The PIN entry can be perceived by close by adversaries, more effectually in a crowded place. A new technique has been established to cope with this problem that is cryptography prevention techniques. Instead, there have been alternative approaches among them, the PIN entry was elegant because of its simplicity and accessibility. The basic BW method is focused to withstand a human shoulder surfing attack. In every round, a well ordered numeric keypad is colored at odd. A user who knows the accurate PIN digit can enter by pressing the separate color key. The IBW method is examined to be confidential against human nemesis due to the restricted cognitive abilities of humans. Also the IBW method is proven to be robust against any hacking attacks.

B. Title: Gaze-Based Password Authentication throughAutomatic Clustering of Gaze Points

Author: Justin Weaver, Kenrick Mock, Bogdan Hoanca

Researchers have proposed systems in which users utilize an eye tracker to enter passwords by merely looking at the proper symbols on the computer monitor in the appropriate order. This authentication method is immune to the practice of shoulder surfing: secretly observing the keystrokes of a legitimate user as heor she types a password on a keyboard. In this paper we describe the EyeDent system—in which users authenticate by looking at the symbols on an on-screen keyboard to enter their password. Existing eye-tracking based.authentication systems require the userto dwell or press a trigger when looking at each symbol.

C. Title: Gaze-Based Password Authentication through Automatic Clustering of Gaze Points

Author: Justin Weaver, Kenrick Mock, Bogdan Hoanca Here researchers have proposed one system i.e eye tracker to enter password by looking at the proper symbol on the computer monitor in an appropriate order. This type of authentication is used in order to avoid shoulder surfing. And in this paper we have discussed the Eye Dent System in which users authenticate by looking at the symbols on an server to enter their password. And in Eye Dent, gaze points are automatically clustered to determine the user selected symbols. Result from this investigation indicates that quick authentication is possible usingthis scheme.

D. Title: Drag-and-Type: A New Method for Typing with Virtual Keyboards on Small Touch screens

Author: Taekyoung Kwon, Sarang Na,and Sang-ho Park Some users are experiencing difficulties and also many errors in typing alphanumeric keys with their thumb. Because small touch screens are widely used in consumer electronics, such as smart phones and mobile electronic devices. However, typing on the small touch screen is still worth studying. In fact, smart phone users are experiencing difficulties and also many errors in typing alphanumeric keys with their thumbs because a small virtual keyboard even with the reduced set of touchable keys can only provide tiny size keys to the users. This paper studies a new style of typing method called Drag and-Type, which leverages the dragging action instead of direct tapping on the touch screen to ease more accurate typing on the small virtual keyboard virtual keyboard can only provide tiny size keys. Drag-and- Type, which provides the dragging action instead of direct tapping on the touchscreen. In existing system we are using keyboard from which the attacker can easily accessible the password by using shoulder-surfing and thermal attacks. Proposed method could be used for secure and accurate password entry.

III. PROPOSED SYSTEM

A. Problem Statement

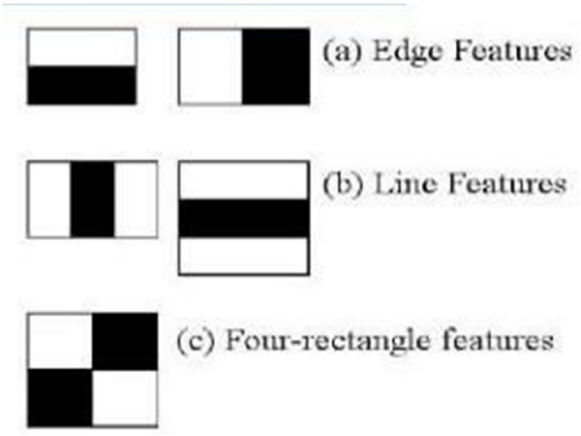
The use of personal identification numbers (PINs) is a common user authentication method for many applications, such as money management in automatic teller machines (ATMs), approving electronic transactions, unlocking personal devices, and opening doors. Authentication is always a challenge even while using PIN authentication. According to European ATM Security, fraud attacks on ATMs increased by 26% in 2016 compared to that of 2015. Authorized user enters the code in public places make PIN entry vulnerable to password attacks, such as shoulder surfing as well as thermal tracking.

B. Methodology

1) *HARR Cascade Face Detection:* Haar Cascade is a machine learning object detection algorithm used to identify objects in an image or video and based on the concept of features proposed by Paul Viola and Michael Jones in their paper "Rapid Object Detection using a Boosted Cascade of Simple Features" in2001. It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. It is then used to detect objects in other images.

The algorithm has four stages:

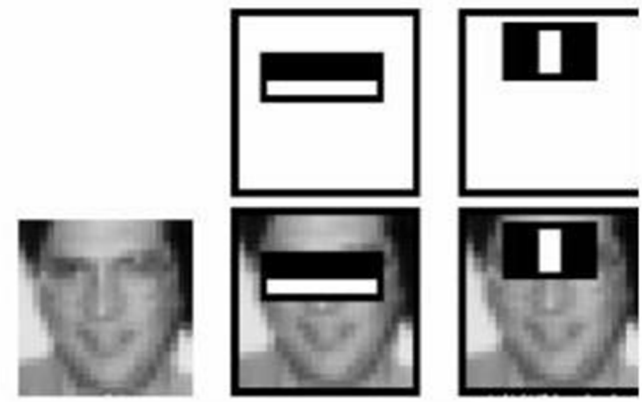
a) *Haar Feature Selection:* First step is to collect the Haar Features. A Haar feature considers adjacent rectangular regions at a specific location in a detection window, sums up the pixel intensities in each region and calculates the difference between these sums.



2) *Creating Integral Images:* Integral Images are used to make this super fast.

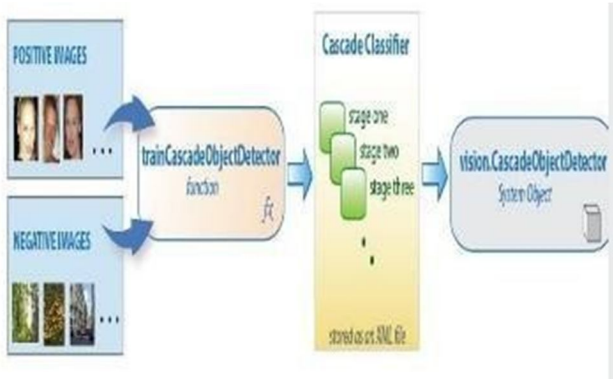
3) *Adaboost Training:* Among all these features we calculated, most of them are irrelevant. For example, consider the image below. Top row shows two good features. The first feature selected seems to focus on the property that the region of the eyes is often darker than the region of the nose and cheeks. The second feature selected relies on the property that the eyes are darker than the bridge of the nose. But the same windows applying on cheeks or any other place is irrelevant.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com



So how do we select the best features out of 160000+ features? This is accomplished using a concept called Adaboost which both selects the best features and trains the classifiers that use them. This algorithm constructs a "strong" classifier as a linear combination of weighted simple "weak" classifiers.

4) Cascading Classifiers



The cascade classifier consists of a collection of stages, where each stage is an ensemble of weak learners. The weak learners are simple classifiers called decision stumps. Each stage is trained using a technique called boosting. Boosting provides the ability to train a highly accurate classifier by taking a weighted average of the decisions made by the weak learners. Each stage of the classifier labels the region defined by the current location of the sliding window as either positive or negative. Positive indicates that an object was found and negative indicates no objects were found. If the label is negative, the classification of this region is complete, and the detector slides the window to thenext location. If the label is positive, the classifier passes the region to the next stage. The detector reports an object found at the current window location when the final stage classifies the region as positive. The stages are designed to reject negative samples as fast as possible. The assumption is that the vast majority of windows do not contain the object of interest. Conversely, true positives are rare and worth taking the time to verify.

- A true positive occurs when a positive sample is correctlyclassified.
- A false positive occurs when a negative sample is mistakenlyclassified as positive.
- A false negative occurs when a positive sample is mistakenlyclassified as negative.

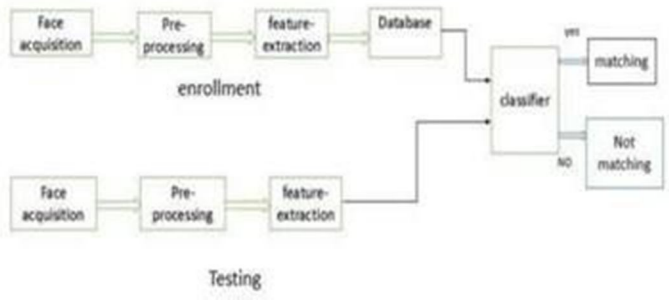
To work well, each stage in the cascade must have a low false negative rate. If a stage incorrectly labels an object as negative, the classification stops, and you cannot correct the mistake. However, each stage can have a high false positive rate. Even if the detector incorrectly labels a nonobject as positive, you can correct the mistake in subsequent stages. Adding more stages reduces the overall false positive rate, but it also reduces the overall true positive rate. Cascade classifier training requires a set of positive samples and a set of negative images. we must provide a set of positive images with regions of interest specified to be used as positive samples. we can use the Image Labeler to label objects of interest with bounding boxes. The Image Labeler outputs a table to use for positive samples. we also must provide a set of negative images from which the function generates negative samples automatically. To achieve acceptable detector accuracy, set the number of stages, feature type, and other function parameters.

5) *LBPH Face Reorganization:* Local Binary Patterns Histogram algorithm was proposed in 2006. It is based on local binary operator. It is widely used in facial recognition due to its computational simplicity and discriminative power.

The steps involved to achieve this are:

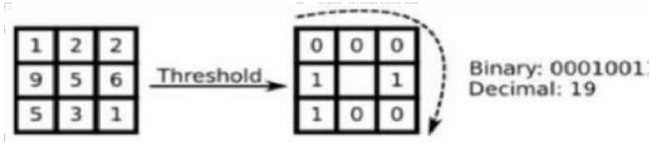
- Creating dataset
- Face acquisition
- Feature extraction
- Classification

The LBPH algorithm is a part of opencv.Steps

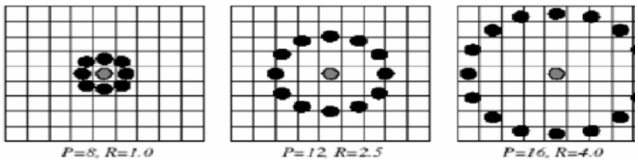


• Suppose we have an image having dimentions N x M.
• We divide it into regions of same height and width resulting inm x m dimension for every region.

• Local binary operator is used for every region. The LBPoperator is defined in window of 3x3.
being the intensity of the the neighbor pixel
Using median pixel value as threshold, it compares a pixel to its8 closest pixels.
• If the value of neighbor is greater than or equal to the centralvalue it is set as 1 otherwise it is set as 0.
•Thus, we obtain a total of 8 binary values from the 8 neighbors.
• After combining these values we get a 8 bit binary numberwhich is translated to decimal number for our convenience.
• This decimal number is called the pixel LBP value and itsrange is 0-255.

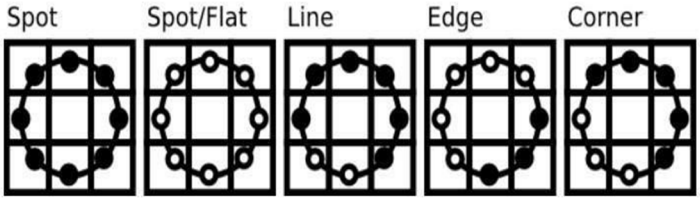


• Later it was noted that a fixed neighborhood fails to encode details varying in scale .The algorithm was improved to use different number of radius and neighbors , now it was known as circular LBP.

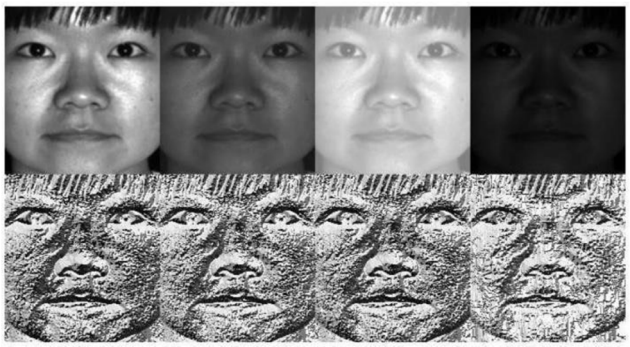


• The idea here is to align an arbitrary number of neighbors on a circle with a variable radius.

This way the following neighborhoods are captured:

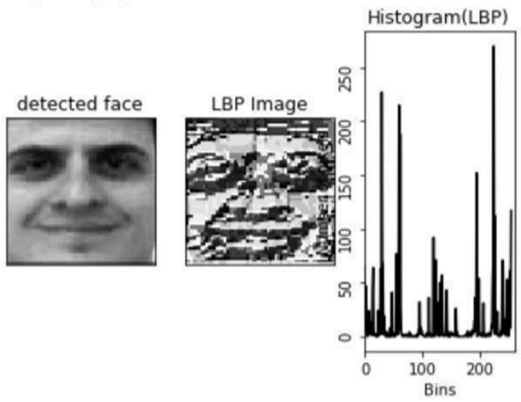


- For a given point (Xc,Yc) the position of the neighbor(Xp,Yp), p belonging to P can be calculated.
- here R is radius of the circle and P is the number ofsample points.
- If a points coordinate on the circle doesn't correspond to image coordinates, it get's interpolated generally by bilinear interpolation.
- The LBP operator is robust against monotonic gray scaletransformations.



• After the generation of LBP value histogram of the region is created by counting the number of similar LBP values in the region.

• After creation of histogram for each region all the histograms are merged to form a single histogram and this is known as feature vector of the image.



• Now we compare the histograms of the test image and the images in the database and then we return the image with the closest histogram. (This can be done using many techniques likeEuclidean distance, chi-square, absolute value etc)

• The Euclidean distance is calculated by comparing the test image features with features stored in the dataset. The minimum distance between test and original image gives the matching rate.

$$d(a,b) = \sqrt{\sum_{i=1}^{n} |a_i - b_i|^2}$$

• As an output we get an ID of the image from the database if the test image is recognised.

LBPH can recognise both side and front faces and it is not affected by illumination variations which means that it is more flexible

IV. COMPARISON

The method for entering passwords can be made safe enough using latest method that is eye blinking .User's can enter the password by blinking the eye at the suitable symbols in the appropriate order which will make the user's is invulnerable to shoulder surfing(observation of user while typing his/her password through the keyboard

A. Proposed System

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 ofpassword 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.

V. FLOWCHARTS

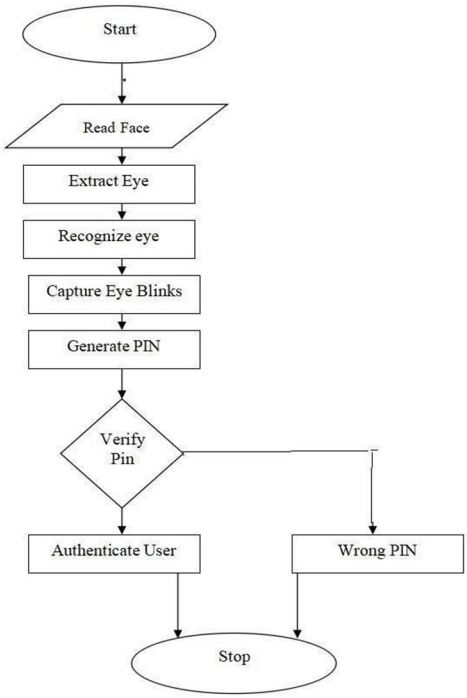


Figure.5.1. System Architecture

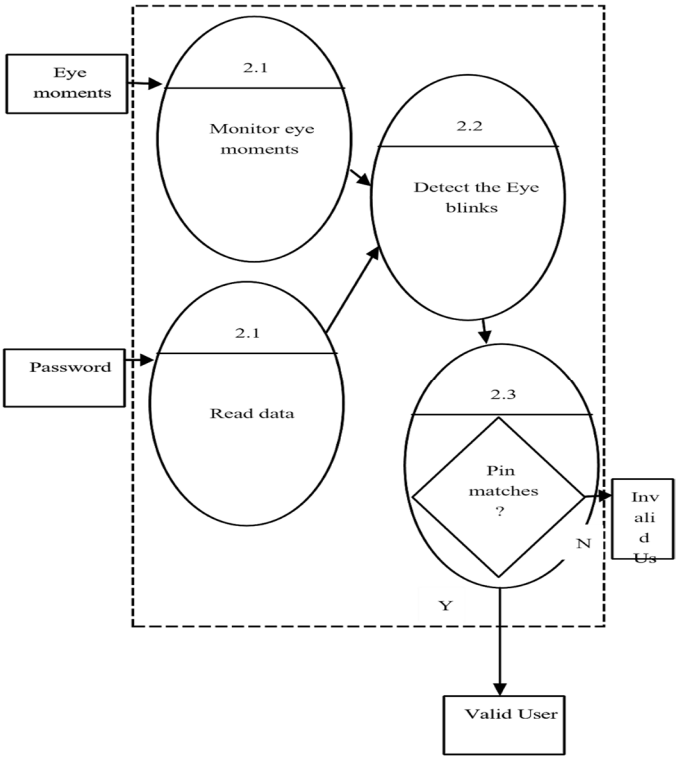


Figure.5.2-Eye password generation and OTP verification

VI. EXPERIMENT

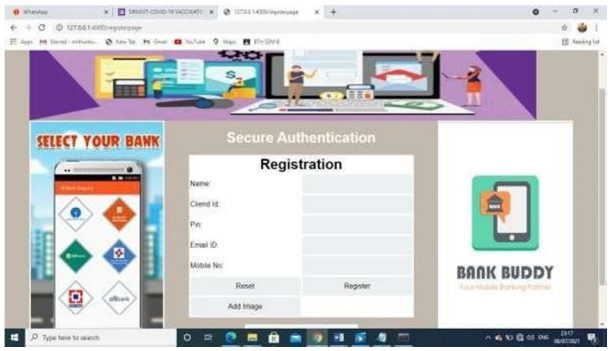


Figure.6.1.User Registration

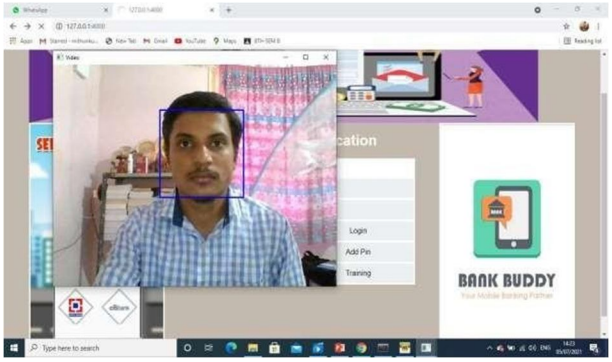


Figure.6.2-capturing of user's picture while registering

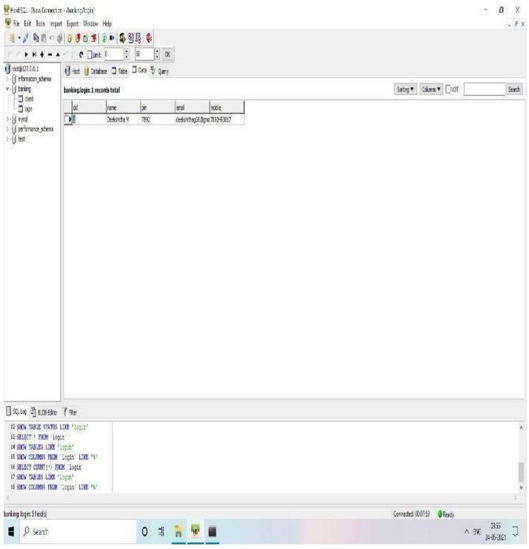


Figure.6.3-Registered user's information stored indatabase

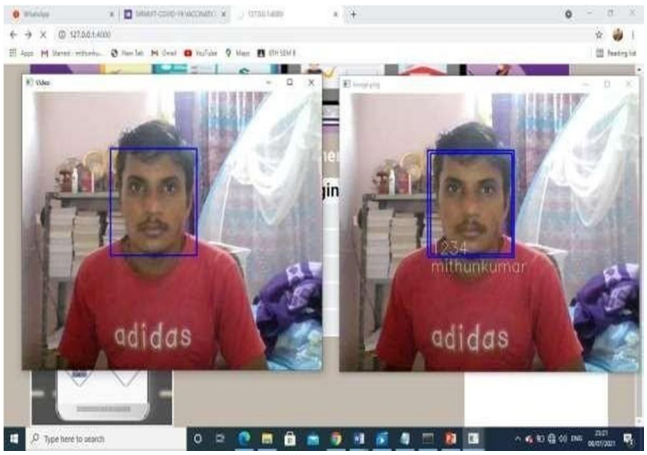


Figure.6.4.Identification of user's face based on the information given while registering with this application

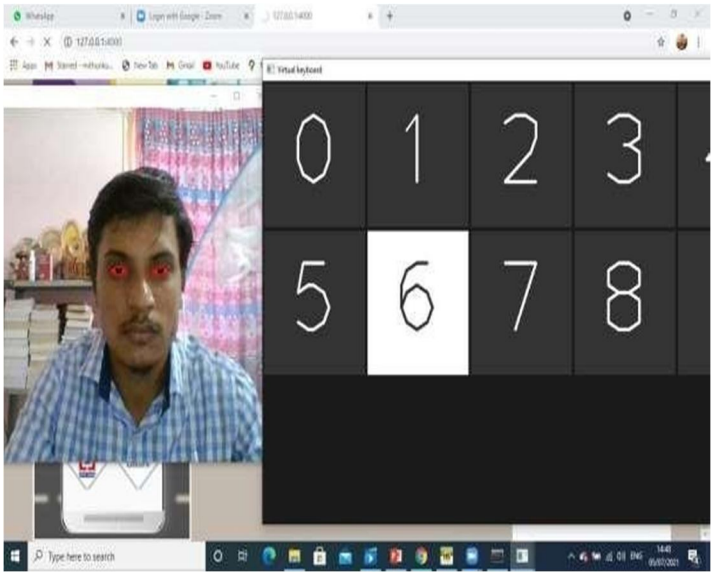


Figure.6.5.virtual keyboard to add pin through eyeblink

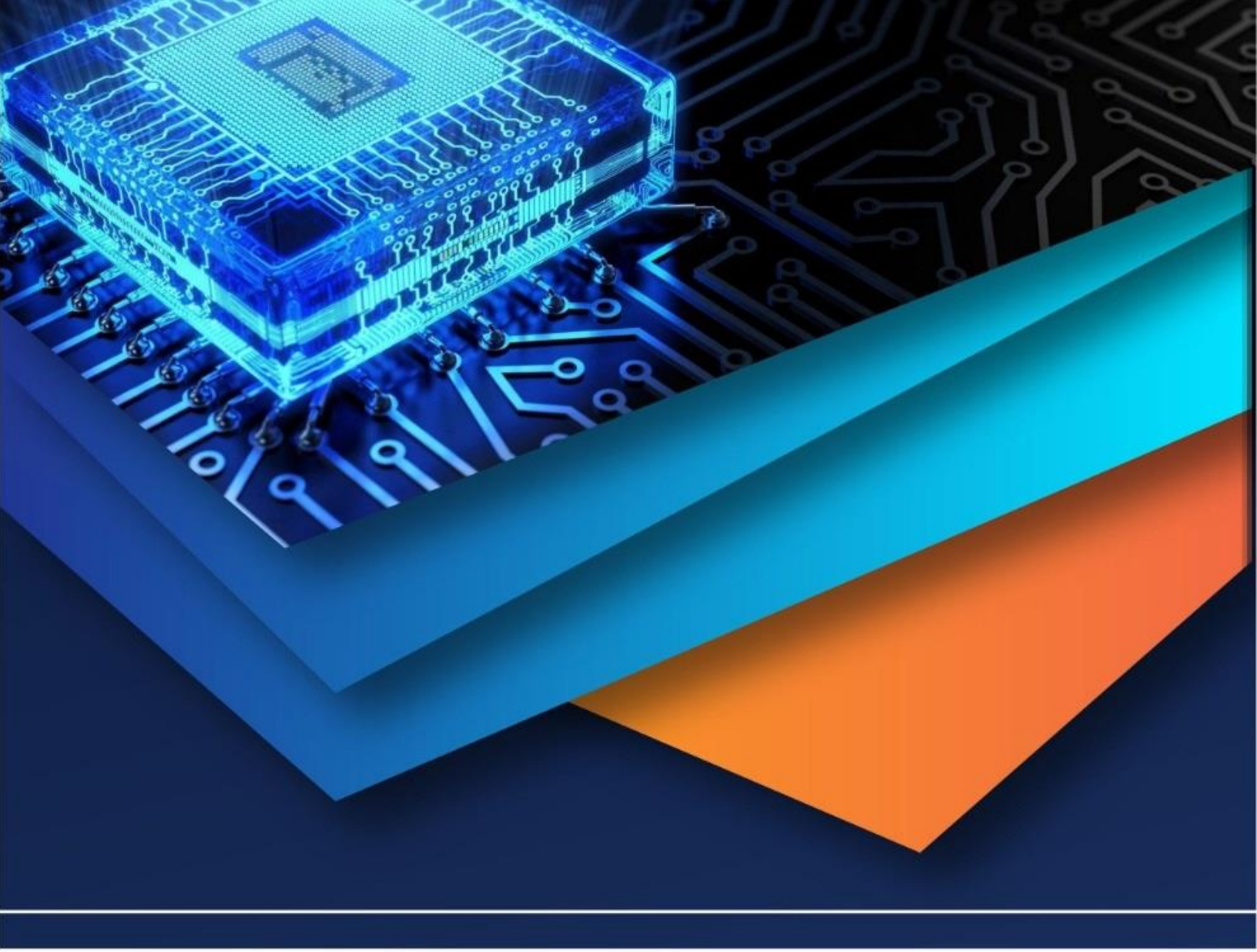
Figure.6.6.OTP verificationFigure.6.7.Login Page

VII. CONCLUSION

A smart-camera based eye-blinking system has been incorporated into a new application for eyelid blinkbased PIN identification, the PIN identification is accomplished after real- time eye-blinks and eye center computations and recording are completed. Leakage of the passwords can be overcome by this method . A smart-camera based eye-blinking system has been incorporated into a new application for eyelid blinkbased PIN identification. The system has been successfully tested with a nine-digit keypad, and can be extended to character and digit combination password entry.. The stability of the user's eye blink will affect the accuracy of the detected pins.

REFERENCES

[1] R. Revathy and R. Bama, "Advanced Safe PIN-EntryAgainst Human Shoulder-Surfing," IOSR Journal ofComputer Engineering, vol 17, issue 4, ver. II. pp. 9-15,JulyAug.2015.(Available:http://www.iosrjournals.org/io sr-jee/papers/Vol17-issue4/Version2/B017420915.pdf) Based Attacks," WOOT '11, pp. 1-8, August 2011.(Available:https://cseweb.ucsd.edu/kmowery/papers/thermadf)
[2] K. Mowery, S. Meiklejohn and S. Savage, "Heat of theMoment: Characterizing the Efficacy of Thermal Camera-
[3] M. Mehrubeoglu, E. Ortlieb, L.. McLauchlan, L. M.
[4] 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(DOI: 10.1109/1CSMC.2011.6084072).
[5] "ATM Fraud, ATM Black Box Attacks SpreadAcross Europe", European ATM SecurityTeam(E.A.S.T.), online, posted 11 April 2017.(Available:https://www.european-at security.eu/tag/atmfraud/) Pham, "Capturing reading patterns throughareal-time smart camera iris tracking system," Proc. SPIE, vol. 8437, id. 843705,2012.(DOI:10.1117/12.922875).
[6] 2018 IEEE International Conference on Consumer Electronics, Mr Kaustubh.S.Sawant, Mr. Pange P.D has published "Real-time eye tracking for password authenticationusing gaze based".
[7] Smart Cameras for Embedded Machine Vision,(product information) National Instruments(Available: http://www.ni.com/pdf/products/us/cat ni 1742.pdf).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY