IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10715

Pin Authentication System Based on Real Time Eye Pupil Tracking

B S Balaji [1], Thejaswini KG[2], Vanishree SV[3], Supritha LR[4]

Department of Electronics and Communication Engineering, B.G.S Institute of Technology, B.GNagara-571448

Abstract: Machine Learning (ML) is a field of artificial intelligence that uses statistical techniques to give computer systems the ability to "learn from data", without being explicitly programmed. Machine learning explores the study and construction of algorithms that can learn from and make predictions on data – such algorithms overcome following strictly static program instructions by making data-driven predictions or decisions, through building a model from sample inputs.

Keywords: Machine Learning (ML), Personal Identification Numbers (PINs), Real Time Eye Pupil Tracking, Virtual Assistants.

I. INTRODUCTION

1.1 Overview

Opportunities of machine learning
Image recognition
Advanced customization
Voice recognition
Intelligent data analysis
Optical character recognition
Sensory data analysis

Figure 1 Opportunities of Machine Learning

1..1Machine Learning Tasks

Machine learning tasks are typically classified into several broad categories:
• Feature Selection: Feature selection is one of the critical tasks which would be used when building machine learning models. Feature selection is important because selecting right features would not only help build models of higher accuracy but also help achieve objectives related to building simpler models, reduce over fitting etc.
• Regression: Regression tasks mainly deal with estimation of numerical values. Some of the examples include estimation of housing price, product price, stock price etc.
• Dimension reduction: Dimension reduction is the process of reducing the number of random variables under consideration and can be divided into feature selection and feature extraction.
• Testing and matching: Testing and matching tasks relates to comparing data sets.

1...2Machine Learning Applications

• Virtual Personal Assistants: Machine learning is an important part of these personal assistants, as they collect and refine the information on the basis of the previous involvement with them. Later, this set of data is utilized to render results that are tailored to specific preferences. Virtual Assistants are integrated to a variety of platforms

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10715

like smart speakers, smart phones, mobile apps. improve the search results. Every time a search is executed, the algorithms at the backend keep a watch at how it responds to the results.

with digital zoom contains the same number of pixels, the detail is clearly far less than with optical zoom. Digital sampling of any signal, whether sound, digital photographs, or other, can result in apparent signals at frequencies well below anything present in the original. Aliasing occurs when a signal is sampled at a less than twice the highest frequency present in the signal. Signals at frequencies above half the sampling rate must be filtered out to avoid the creation of signals at frequencies not present in the original sound. Thus, digital sound recording equipment contains low-pass filters that remove any signals above half the sampling frequency.

Since a sampler is a linear system, then if an input is a sum of sinusoids, the output will be a sum of sampled sinusoids. This suggests that if the input contains no frequencies above the Nyquist frequency, then it will be possible to reconstruct each of the sinusoidal components from the samples. This is an intuitive statement of the Nyquist-Shannon sampling theorem. Anti-aliasing is a process which attempts to minimize the appearance of aliased diagonal edges. Anti-aliasing gives the appearance of smoother edges and higher resolution. It works by taking into account how much an ideal edge overlaps adjacent pixels.

1..3 RFID Reader and Tags

RFID Reader is used to read information which is stored in RFID tag. This reader operated on 125 KHz which contain on-chip antenna which can be powered with 5V power supply. Reader is attached to a computer or any microcontroller in the system and then connected it to the computer through which it communicates with computer devices. Communication range of reader is 2-10 cm. Tags contain the information which is read when it is tap on the reader.

1..4 Haar Cascade Algorithm

Haar-cascade is an object detection algorithm used to locate faces, pedestrians, objects and facial expressions in an image, and mainly used for face detection. In Haar-cascade, the system is provided with several numbers of positive images (like faces of different persons at different backgrounds) and negative images (images that are not faces but can be anything else like chair, table, wall, etc.).

1..5 Features of Haar

A more sophisticated method is therefore required. One such method would be the detection of objects from images using features or specific structures of the object in question. However, there was a problem. Working with only image intensities, meaning the RGB pixel values in every single pixel in the image, made feature calculation rather computationally expensive and therefore slow on most platforms. This problem was addressed by Haar-like features, developed by Viola and Jones. A Haar-like feature considers neighboring 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. This difference is then used to categorize subsections of an image. An example of this would be the detection of human faces. Commonly, the areas around the eyes are darker than the areas on the cheeks. One example of a Haar-like feature for face detection is therefore a set of two neighboring rectangular areas above the eye and cheek regions.

1..6 Cascade Classifier

The cascade classifier consists of a list of stages, where each stage consists of a list of weak learners. The system detects objects in question by moving a window over the image. Each stage of the classifier labels the specific region defined by the current location of the window as either positive or negative – positive meaning that an object was found or negative means that the specified object was not found in the image. If the labelling yields a negative result, then the classification of this specific region is hereby complete and the location of the window is moved to the next location. If the labelling gives a positive result, then the region moves of to the next stage of classification. The classifier yields a final verdict of positive, when all the stages, including the last one, yield a result, saying that the object is found in the image. A true positive means that the object in question is indeed in the image and the classifier labels it as such – a positive result. A false positive means that the labelling process falsely determines that the object is located in the image, although it is not. A false negative occurs when the classifier is unable to detect the actual object from the image and a true negative means that a non-object was correctly classifier as not being the object in question. In order to work well, each stage of the cascade must have a low false negative rate, because if the actual object is classified as a non-object, then the classification of that branch stops, with no way to correct the mistake made. However, each stage can have a relatively high false positive rate, because even if the n'th stage classifies the non-object as actually being the object, then this mistake can be fixed in n+1-th and subsequent stages of the classifier.

1..7 About The Project

The use of PINs as passwords for authentication is ubiquitous nowadays. This is especially true for banking applications where the combination of a token (e.g. bank card) and the user's secret PIN is commonly used to authenticate transactions. In financial applications PINs are typically four-digit numbers, resulting in 10000 possible numbers. The security of the system relies on the fact that an attacker is unlikely to guess the correct PIN number and that the systems (e.g., Automated Teller Machines) limit the user to few attempts (e.g., 3) for entering the correct PIN. As most applications that use PINs for authentication operate in a public setting a common attack is to try to observe and record a user's PIN entry (shoulder-surfing).These security problems have been recognized for a long time and researchers have proposed a number of different schemes to minimize the risk of PIN entry observation. One such proposed alternate PIN entry method requires the user to input some information, which is derived from a combination of the actual PIN and some additional information displayed by the system, instead of the PIN itself. Another approach proposes the use of an elaborate hardware to make PIN entry resilient to the observation attacks. However, these method has not been introduced into practical applications because the users would have to be retrained to use a completely different approach to PIN entry and the significant additional costs involved in the hardware setup.

1.2 Problem Statement

Password authentication using PINs requires user to physically input the PIN .Entering the PIN in public places makes it vulnerable to password attacks such as shoulder surfing and thermal tracking. To overcome this problem, hands-off gaze based PIN entry and Haar cascade algorithm for PIN identification using camera is proposed.

1.3 Objectives

- Designing a system for tracking face and eye using camera.
- Providing authentication for PINs.
- Achieving synchronization between image processing and the systems.
- To protect the users from shoulder-surfing in ATMs.

1.4 Introduction

With the invention of the computer in the middle of the last century there was also the need of an interface for users. In the beginning experts used teletype to interface with the computer. Due to the tremendous progress in computer technology in the last decades, the capabilities of computers increased enormously and working with a computer became a normal activity for nearly everybody. With all the possibilities a computer can offer, humans and their interaction with computers are now a limiting factor. This gave rise to a lot of research in the field of HCI (human computer interaction) aiming to make interaction easier, more intuitive, and more efficient. Interaction with computers is not limited to keyboards and printers anymore. Different kinds of pointing devices, touch-sensitive surfaces, high-resolution displays, microphones, and speakers are normal devices for computer interaction nowadays. There are new modalities for computer interaction like speech interaction, input by gestures or by tangible objects with sensors. A further input modality is eye gaze which nowadays finds its application in accessibility systems. Such systems typically use eye gaze as the sole input, but outside the field of accessibility eye gaze can be combined with any other input modality. Therefore, eye gaze could serve as an interaction method beyond the field of accessibility. One of the security requirements for general terminal authentication systems is to be easy, fast and secure as people face authentication mechanisms every day and must authenticate themselves using conventional knowledge-based approaches like passwords. But these techniques are not safe because they are viewed by malicious observers who use surveillance techniques such as shoulder-surfing (observation user while typing the password through the keyboard) to capture user authentication data. Also there are security problems due to poor techniques such as shoulder-surfing (observation user while typing the password through the keyboard) to capture user authentication data. Also there are security problems due to poor interactions between systems and users. As a result, the researchers proposed eye tracking systems, where users can enter the password by looking at the suitable symbols in the appropriate order and thus the user is invulnerable to shoulder surfing. Eye tracking is a natural interaction method and security systems based on eye movement tracking provide a promising solution to the system security and usability.

1.5 Literature Survey

The study of existing security systems that are based on eye movement tracking developed by different researchers according to their area of expert. In the following paragraphs are given several of the published researches related to the goals of this work.

DOI 10.17148/IJARCCE.2021.10715

2.2.1 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.
In computer security, shoulder surfing refers to using direct inspection techniques, such as peeping over someone's shoulder, to acquire information. Shoulder surfing is frequently used to acquire passwords, PIN security codes, and related data. To stop shoulder surfing, which is between the customer and the system, cryptographic prevention approach is hardly relevant because users are restricted in their capacity to process information. Among them, the PIN entry technique introduced was effective because of its clarity and instinctive in every round, a structured numeric keypad is colored at odd half of the keys are in black and another half in white, which is called as BW method. A customer who knows the accurate PIN digit can enter the color by pressing the distinct color key below. The primary BW method is targeted to withstand a human shoulder surfing attack. [1]

Advantages

- It reduces the difficulties of shoulder surfing or eves dropping by introducing the different PIN entry methods.
- BW method is used for PIN entry which provides security and usability.
- It provides high usability and gives compatibility and cost effectiveness.

II. LIMITATIONS

BW method is aimed to resist a human shoulder surfing attack. But if the selected halves were memorized or written on a paper, consecutive rounds and recalled to derive their grouping pattern, the shoulder surfer could identify a single digit of the PIN.

2.2.2 Mohamed, Florian, Mariam, Emanuel, Regina and Andreas "Gaze-Touch Pass Scheme". The 34th ACM SIGCHI Conference on Human Factors in Computing Systems CHI 2016, At San Jose, CA, USA. May 2016
With mobile devices enabling ubiquitous access to sensitive information, there is a need to protect access to such devices. Meanwhile, authentication schemes are prone to shoulder surfing attacks, where a bystander observes a user while authenticating. The attacker then gets hold of the device and tries to authenticate and access sensitive data. To overcome this attacks Gaze Touch Pass, a multimodal authentication scheme in which user define four symbols, each can be entered either via touch (a digits between 0 and 9) or via gaze (gazing to the left and to the right). Consecutive gaze inputs to the same direction would then need to be separated by a gaze to the front and switches between input modalities are used within a single password.

Advantages

- Gaze Touch Pass is particularly secure against side attack.
- Gaze Touch Pass achieves a balance between security and usability, with low authentication times and high observation resistance.
- Gaze Touch Pass is faster and can work on off-the-shelf mobile devices without additional hardware.
- Gaze Touch Pass shows that multimodal passwords are significantly more secure than single modal ones.

Limitations

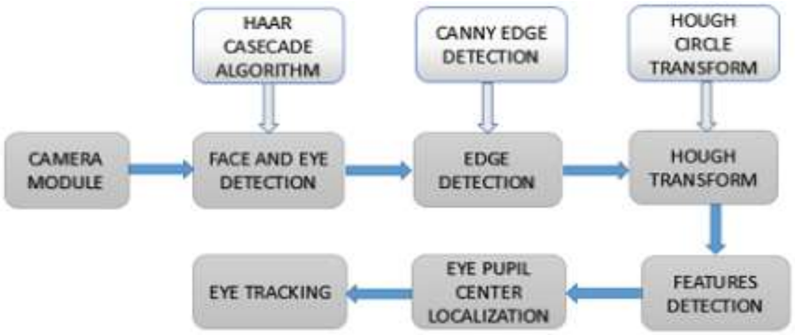
- It's applicable only for mobile devices.
- Gaze Touch Pass can be particularly useful as a secondary authentication mechanism that users can choose to opt to when feeling observed (e.g. public setting),or when accessing critical data (e.g. online banking).

III. METHODOLOGY

The principle of this system is eye pupil detection and eye tracking based on computer vision technology. A new algorithm introduced for detecting the eye pupil location by Image processing. In this technique, several stages are used to find out the movement of eye, such as face detection, eye detection, edge detection, hough transformed, motion detection and object tracking. During the initial stage, the system captures the images by web camera. The first step is to detect the user face. A system indicates and represents the face of user in a specific area of image. After that, system will perform several operations of image processing to track the eye pupil.

The figure 2.1 represents the complete methodology of proposed system. Firstly, the camera will capture the image and then the face detection takes place. After the detection of the face, the the eye on the face are detected, which is a region of interest.

The systems will corp the eye region initially and it will detect the eye center point. Corner detection method is applied to find out the regions of eye corners. The distance between the eye region corner and eye pupil center are measured using coordinates system logic. According to the eye pupil movements, the distance measured will vary. A minimum distance indicates the eye pupil is moved towards the left, and maximum values indicates the eye moved on right and if there is no movements of the eye, then it concludes that eye is in the middle position. After tracking the eye pupil position, the data is taken by the system. The entered data is compared with the trained dataset. If the entered data is not matched with the trained data then the system will display an error message as "unauthorized access" else the system confirms and allows for further transaction.



System Processing

IV. SUMMARY

The personal identification numbers (PINs) is a common user authentication method for many applications, such as money transactions in automatic teller machines (ATMs), unlocking personal devices and opening doors. Authentication remains a challenge even when user enters a PIN in open or public places, makes PIN entry vulnerable to password attacks, such as shoulder surfing as well as thermal tracking. To overcome this problem, hands-off gaze-based PIN entry technique is used, which leaves no footprints behind. Gaze-based authentication refers to finding the eye location across sequential image frames and tracking eye center. Haar Cascade algorithm is a machine learning approach used for detecting the eye pupil location by Image Processing. In this technique, several stages are used to find out the movement of eye, such as Face detection and Eye detection, Edge detection. The distance between the center point and eye pupil center are measured using coordinates system logic. According to the eye pupil movements, the measured distance will vary. A minimum distance indicates the eye pupil is moved towards the left, and maximum values indicates the eye moved on right and if there is no movements of the eye, then it concludes that eye is in the middle position. After tracking the eye pupil position, the data is taken by the system. The entered data is compared with the trained dataset. If the entered data is not matched with the trained data then the system will throw an error as "unauthorized access" else the system confirms and allows for further transaction.

SYSTEM ANALYSIS

4.1 Introduction

Project requirements are conditions or tasks that must be completed to ensure the success or completion of the project. They provide a clear picture of the work that needs to be done. They are meant to align the project resources with the objectives of the organization. The benefits of effectively gathering project requirements include cost reduction, higher project success rates, more effective change management and improved communication among stakeholders.

Any coherent and reasonable project must have requirements that define what the project is ultimately supposed to do. A requirement is an objective that must be met. Planners cast most requirements in functional terms, leaving design and implementation details to the developers. They may specify price, performance and reliability objectives in fine detail, along with some aspects of the user interface. Sometimes, they describe their objectives more precisely than realistically project requirements provide an obvious tool for evaluating the quality of a project, because a final review should examine whether each requirement has been met unfortunately, it is never quite that easy. Requirements tend to change through the course of a project, with the result that the product as delivered may not adhere to the available requirements this is a constant and annoying facet to the quality assurance process. Moreover, meeting all of the requirements does not ensure a quality product, since the requirements may not have been defined with an eye towards the quality of the end-user is experience.

3.2.3 **Hardware requirements**

• Processor : Pentium IV 2.4 GHz

• Hard disk : 16 GB

• RAM : 4 GB

• Input devices : Web Camera

• RFID card and RFID card reader

• Power Supply
(Any desktop/Laptop with above configuration or higher level)

3.2.4 **Software requirements**

• Operating system : Linux

• Coding language : Python 2.7

• Library : Open CV

9.1 Block Diagram

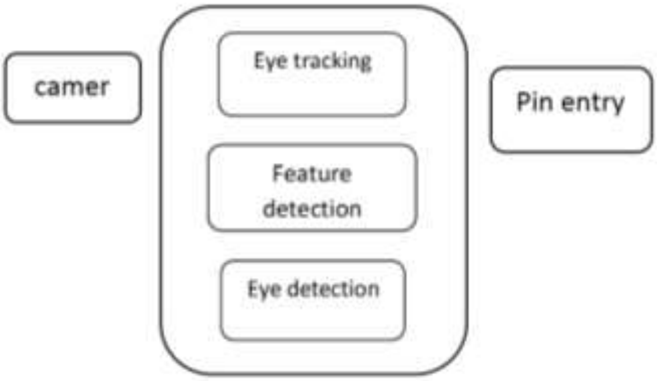


Figure 3.1 Block Diagram of Eye tracking System

9.1.1 Web camera

A webcam is a video camera that feeds or streams its image in real time to or through a computer to a computer network as shown in figure 3.1 When "captured" by the computer, the video stream may be saved, viewed or sent on to other networks travelling through systems such as the internet, and e-mailed as an attachment. When sent to a remote location, the video stream may be saved, viewed or on sent there. Unlike an IP camera(which connects using Ethernet or Wi-Fi), a webcam is generally connected by a USB cable, or similar cable, or built into computer hardware, such as laptops.

Figure 3

Web camera

9.1.2 Eye detection

Eye will be detected from the images that are captured from the web camera and Haar cascade algorithm is used to detect the eye and corp the eye region.

9.1.3Feature detection

Feature detection takes input from the eye detection module as a Haar classifier to locate the coordinate points for the eye pupil position, then gaze values will be calculated.

9.1.4Eye tracking

Eye blink ratio is calculated and the corresponding number from the keyboard is updated as pin and sent for further authentication process.

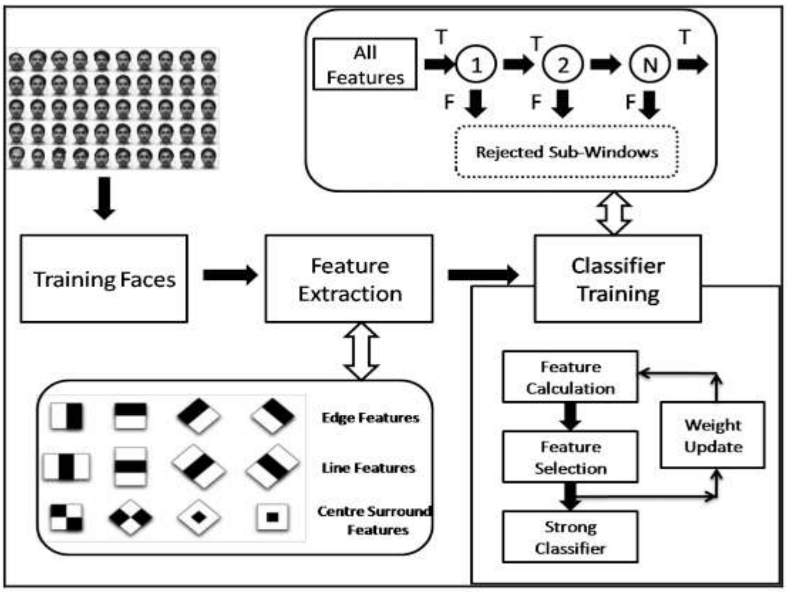


Figure 5 System design of Eye tracking System

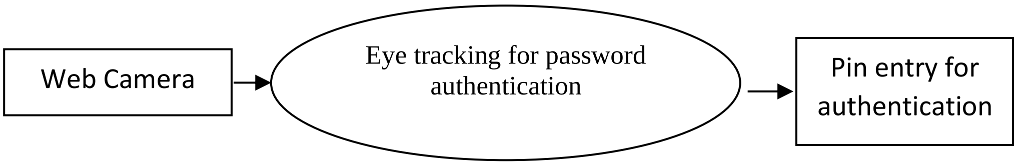

Web Camera
Eye tracking for password authentication
Pin entry for authentication

Figure 4.2 DFD Level 0 Level 1

Figure 4.2 shows some of the detailed modules that are used in eye tracking system. Gaze based pin entry system is divided into three modules as eye detection, feature detection, eye tracking. In eye detection module eye will be detected from the images that are captured from the web camera and Haar cascade algorithm is used to detect the eye. Next module is Feature detection takes input from the eye detection module as a Haar classifier to locate the coordinate points for the eye pupil position, then gaze values will be calculated. Last module is eye tracking in which eye blink ratio is calculated and the corresponding number from the keyboard is updated as pin and sent for further authentication process. Each modules deals with one or more data flows to or from an external agent and which together provide all functionality of the system as a whole. It also identifies the internal data stores that must be present in order for the system to do its job and flow of data between the various inputs of the system. The level 1 DFD for the proposed system is shown in Figure 4.3

6 Haar Cascade Algorithm

Haar Cascade is a machine learning object detection algorithm used to identify objects in an image or video. 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.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10715

26.2RESULTS

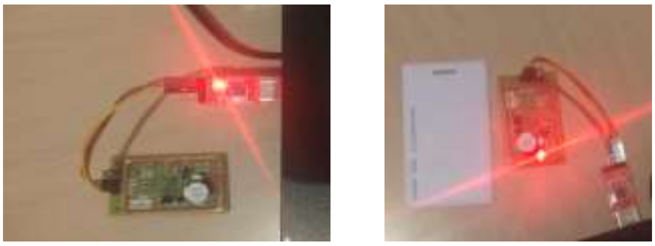
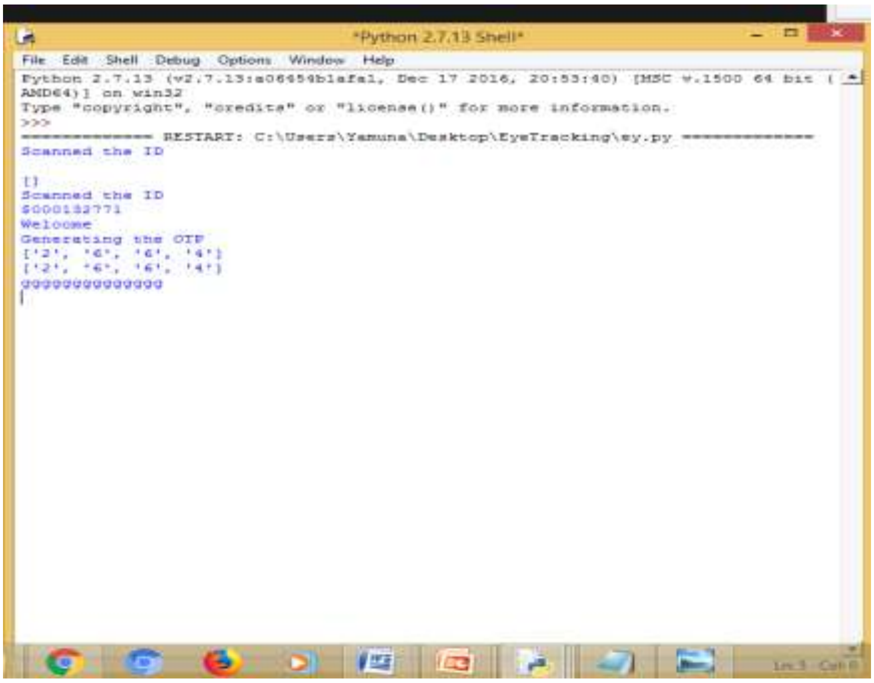


Figure 6.1 RFID reader and RFID card

Fig 6.1 shows the hardware component of RFID reader and card. RFID is used to scan the card to generate OTP.



```
Python 2.7.13 (v2.7.13:a06454b1afa1, Dec 17 2016, 20:53:40) [MSC v.1500 64 bit (
AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
============== RESTART: C:\Users\Yamuna\Desktop\EyeTracking\ey.py ==============
Scanned the ID

[]
Scanned the ID
$000132771
Welcome
Generating the OTP
['2', '6', '6', '4']
['2', '6', '6', '4']
ggggggggggggggg
```

Figure 6.2 Generating OTP.

Fig 6.2 showing the result of generating of OTP. In this user scans a RFID card through RFID reader to get OTP for the specific card.

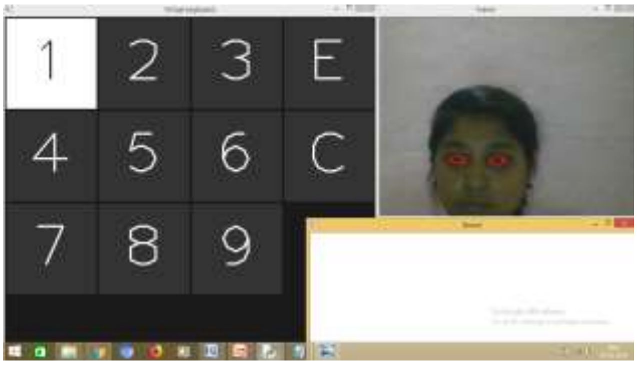


Figure 6.3 Facial image is recognized through web cam, then virtual keypad.

|Fig 6.3 shows virtual keypad along with facial image. In this user facial image is recognized through web cam, if the facial image is not recognized then virtual keypad is not displayed on the screen. If facial image is recognized then virtual keypad is displayed on the screen along with the frame where facial image is cropped with eye region denoted by red color.

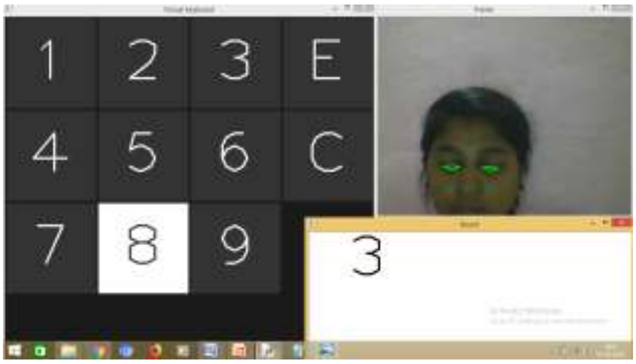


Figure 6.4 Virtual keypad taking input through eyes.

Fig 6.4 shows virtual keypad along with facial image. In this user facial image is recognized through web cam, once the facial image is recognized then virtual keypad is displayed on the screen. If the eye movement is recognized by virtual keypad then the eye region denoted by green color to enter the pin.

software system meets requirements. In this chapter five different test cases of the proposed system have been tested and it is found that the test cases are passed without any problem successfully. In the result section all the test cases have been demonstrated using screenshots. In the performance evaluation section of this chapter the time required for registration and login process is analysed and also the accuracy is evaluated.

V. CONCLUSION

In order to protect the users from shoulder-surfing in ATMs while entering the PIN, new method of entering the PIN are being evaluated. With the eye interaction for PIN entry is emerging as a practical solution. Here we have discussed Safety PIN, which proposes retrofitting the ATMs with an eye tracking device, so that users can enter their PIN without using keypad for pin entry. In our prototype, we have implemented and evaluated the system for PC. In addition to look and shoot and gaze activation methods, by introducing a new activation method called blink activation. Initial user evaluations have yielded encouraging results, prompting further work.

BIOGRAPHIES

Mr. B.S Balaji, Asst. professor, Dept. of ECE, ACU, BGSIT, BG Nagar

Thejaswini KG, Studying B.E (Electronics and Communication Engineering) at B.G.S Institute of Technology

Vanishree SV, Studying B.E (Electronics and Communication Engineering) at B.G.S Institute of Technology

Supritha LR, Studying B.E (Electronics and Communication Engineering) at B.G.S Institute of Technology