IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86122

Password Authentication Provided by Three-Layer Security Using Machine Learning

Preetham G[1], Sandarsha H.M[2], Vineeth S[3], Vipruth L.M[4], Ms. Mouna K.M[5]

Student, Electronics and Communication, BGS Institute of Technology, Mandya, India[1]

Student, Electronics and Communication, BGS Institute of Technology, Mandya, India[2]

Student, Electronics and Communication, BGS Institute of Technology, Mandya, India[3]

Student, Electronics and Communication, BGS Institute of Technology, Mandya, India[4]

Assistant Professor, Electronics and Communication, BGS Institute of Technology, Mandya, India[5]

Abstract: Security of personal devices, bank accounts and Digi-locker, etc. are always given high priority in every human life, the security of these things are accomplished using Personal identification numbers and password. In current day to day life we are complete depend on entering the pin via their hands on a keyboard but this method is not completely safe because the chance of knowing the password by others are more in this case, someone who is standing behind user while user entering the password can easily see what user is typing on a keyboard, this method is known as shoulder surfing and also using thermal detection someone having this thermal detection device can easily crack the entered password or PIN by looking at the keyboard. This two methods i.e., shoulder surfing and thermal tracking are the major drawbacks of entering password or PIN on a keyboard, to overcome these drawbacks this paper proposes a method of entering the PIN using below steps

1. Face detection
2. PIN entry by blinking eyes
3. One Time Password(OTP)

Keywords: User authentication, OTP (one-time password), Haar Cascade, LBPH, Eye blink PIN entry, Face detection, Face recognition.

I. INTRODUCTION

Password or PIN entry authentication are commonly used to verify the identity of an individual who is trying to login or access to a device and this authentication process should be highly secure, accurate and also it should be faster to provide a smooth user experience. These Pin or Password entry methods are being implemented all over the world to ensure the security of personal devices, Bank accounts, ATM and Digi-Lockers, in all these areas users has to enter the PIN or Password using the old methods i.e., entering the password or PIN via hands on a keyboard, but this method is not completely safe as there is a fear a data theft by others while entering the password. These data theft or PIN identification by others can take place through many ways i.e., using shoulder surfing and using thermal tracker to know the hand prints of user who entered the password earlier and with these prints someone can easily trace the PIN or Password entered earlier.

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

Authors: Ms. R Revathy, Mrs. Bama2

Abstract: To prevent the data theft (PIN and Password) in a public place, a new method of entering the PIN or Password is introduced in this paper. The new method invented to enter the pin securely is known as Cryptography prevention strategies. This strategy mainly focuses on entering the PIN with the help of colour key. A unique colour keypad is displayed and the individual or user who knows the exact PIN can enter the PIN. The major advantages of this project is it avoids the shoulder surfing by introducing a new keypad technique. But still this is a drawback because it will not completely avoid shoulder surfing as the keypad is larger and someone who is standing beside user can see the password or PIN entered by the User.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86122

2. Title: Gaze-Based Password Authentication through Automatic Clustering Of Gaze Points
Author: Justin Weaver, Kenrick Mock, Bogdan Hoanca.
Abstract: This advance technique of entering the PIN or Password prevent the shoulder surfing almost completely. This technique is based on simple clustering method to cluster gaze points. The major disadvantage of this project is that the clustering accuracy is less than 83% and PIN generation accuracy is also very less and to implement this technique we need an external camera which is considerably high in rate, so the project is more expensive as it not fit in less budget.

3. Title: Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks
Authors: Keaton Mowery, Sarah Meiklejohn and Stefan Savage
Abstract: This paper discusses about how we can recover the data entered by the user after sometimes using the thermal camera based approach. Once user types his password the button where he pressed while entering PIN or Password have a small prints using this small prints present on the keyboard someone can easily trace the PIN entered by the user or any individual. One more disadvantage of this method is we can get the password or PIN entered by the user in later time before another User types in there.

III. OBJECTIVES

- To present an authentication system to a user which is completely preventing shoulder surfing.
- The main objective is to completely get rid of thermal tracking attack
- To make sure that users are provided with three-layer security while authenticating.

IV. WORKING

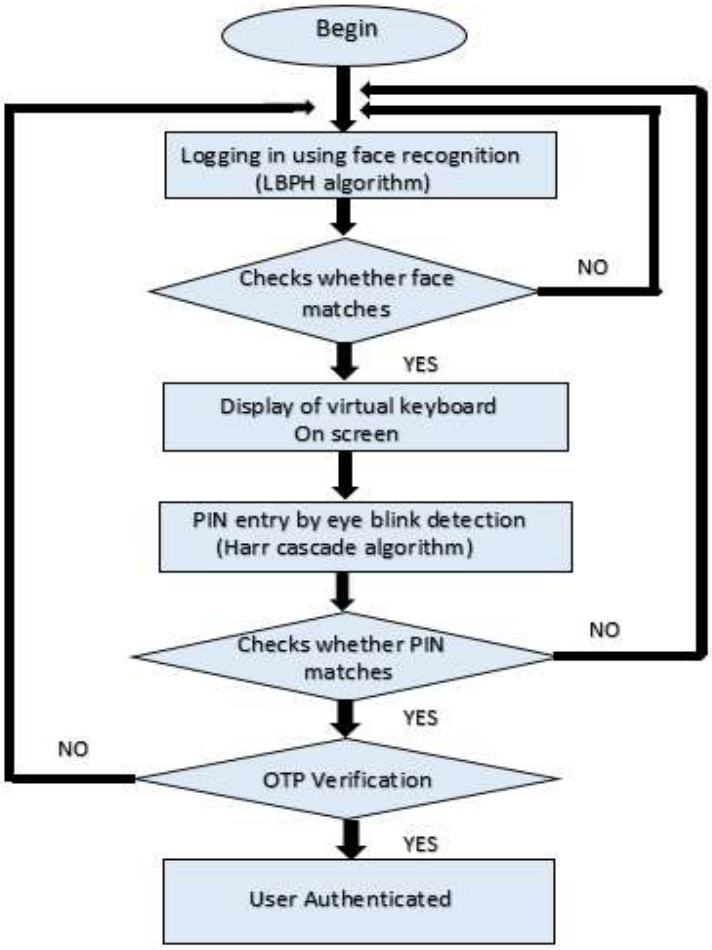

Fig 1: Workflow of Project

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86122

Image Capturing and Facial Recognition

Image capturing and facial recognition of an individual who is trying to authenticate is the crucial step in this project. As a first step of authentication user must register to the system. During the registration process the model is going to capture the image of a user in a continuous video this will be accomplished using OpenCV models. One of the OpenCV feature is used to capture the face of a user and the feature is called Haar Cascade feature.

Haar Cascade

Haar Cascade is a machine learning object detection algorithm used to identify objects in an image or video.
The algorithm has four stages:

- Haar Feature Selection
- Creating Integral Images
- Adaboost Training
- Cascading Classifiers

The Haar cascade has mainly three features they are two rectangle feature, three rectangle feature and four rectangle feature. These features helps to find out the edges, dots or lines in an image. For a given image we cannot apply all these features as it will be hectic for even a high performance computer so keeping that in mind we are creating an integral image from the original image so that the complexity will reduce and also it is easy to find facial feature from the integral image.Third step in haar cascade is using a technique called Adaboost where an integral image pixels are given as an input and it selects features, the classifiers are trained to get the best out of that features. Finally, images are fed to cascade classifiers consists of collection of stages, the stages reject negative samples and outputs all positive samples.

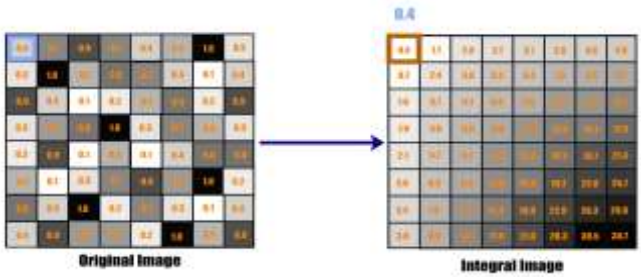

Fig 2: Creating an Integral Image

Local binary pattern histogram (LBPH)

As humans we perform face recognition or face classification every day and every moment of our life. But it may seem easy for the humans while it is quite difficult for the computer. As humans in order to recognize someone we first have to meet the person or see him for the first time so that the face of the person gets stored in our memory. In computer language we can call it as data set. Then when we meet the person again next time our brain compares the current image with the previously stored ones in our memory and then it recognizes the person. similarly in face recognition system when the user comes in front of the camera the computer first has to detect the face from the input image, which is achieved by harr cascade classifier (note: face recognition is different from face detection). After detecting the face to recognize it we use LBPH. LBPH is a simple yet effective texture operator assigns values to the pixels of an image by thresholding neighbour of each pixel then finally considers the results as a binary number. The LBPH is carried out in following steps:

- First, we need to train the algorithm. To achieve it, we need to use a dataset with the facial images of the people we want to recognize.
- We also need a unique ID for each person, so that the algorithm uses it to recognize the input image and give it as the output.
- First computational step of LBPH is to create an intermediate image from the original image. This is done in order to describe the original image in a better way, by highlighting the facial characteristics.
- In order to achieve this the algorithm uses a sliding window on the basis of the parameters radius and neighbours.

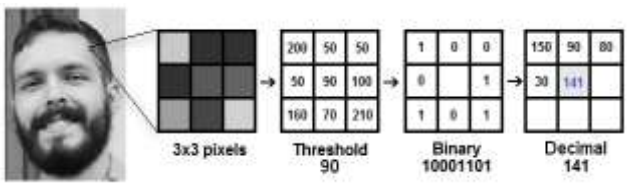

Fig 3: LBPH matrix formation

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86122

- Fist we obtain the image of face in grayscale values.
- Later we obtain the part of the image as 3x3 matrix. It can also be called as 3x3 matrix containing the pixel values in the range 0-255.
- Later we consider the centre value of the matrix as i_c, which is used for thresholding the neighbouring values of the matrix to assign a new value based on the i_c.
- For each neighbouring value of the matrix we assign a new binary number as 1 if the value is higher than the i_c else to 0 if the value is lesser than i_c.
- Now the matrix only contains binary values except the i_c value.
- Later we have to concatenate the each binary value starting from a position to end and generate a new binary number. This binary number is converted to decimal and assigned to the centre value that is i_c.
- Same procedure is performed on each and every pixels in a facial image. At the end we obtain a new image which contains better information than the original image.
- Later this image is converted into histogram based on the pixels values convert complete image to histogram.
- In order to recognize the face, the histogram of the input image is compared with histogram of the dataset based on different approaches such as Euclidean distance, chi-square, absolute value, etc.
- In our project we have used Euclidean distance based approach to identify closely related images.
- The algorithm returns the id of the image with least Euclidean distance than other images.

Eye Blink Detection

To detect eye blink we consider the metric Eye Aspect Ratio (EAR), which is a basic metric to detect and count number of eye blinks from a live video stream. Input facial image consists of different features like eyes, nose, ears, jawline, etc. From these features with help of Harr cascade classifier we extract eye feature, which is the only feature required for eye blink detection.

- Each eye is divided into 6 (x, y) co-ordinates. Starting from the left corner of the eye to remaining in clockwise direction.

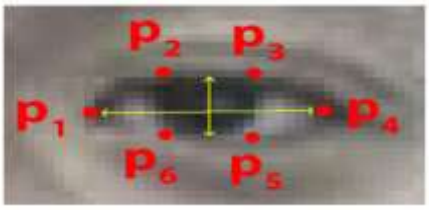

Fig 4: 6(x, y) co-ordinates of eye

- Based on these co-ordinates the Eye Aspect Ratio (EAR) is given as,

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

- Here the numerator of the equation gives the distance between the vertical co-ordinates of the eye while the denominator computes the distance between horizontal co-ordinates of the eye.
- This EAR remains approximately constant throughout the video stream but immediately falls to 0 when there is eye blink occurred.

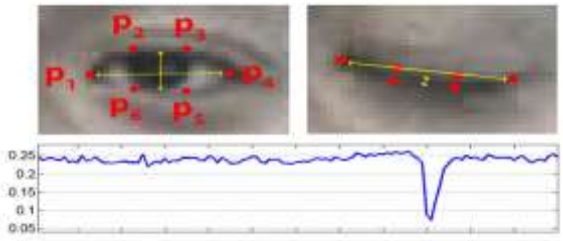

Fig 5: Eye blink detected plot

- Hence when EAR is approximately equal to 0 we can consider that the eye blink has occurred.

OTP Verification

PyOTP is a Python library used for generating and verifying one-time passwords. It can be used to achieve 2FA (two factor) or MFA (multi factor) authentication in different logging in systems and web applications. In our project we have

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86122

used PyOTP to generate OTP's. These OTP's are sent to the user's mobile number with the help of Fast2sms API. After receiving the OTP the user has to enter the received OTP in order to authenticate into the system.

V. RESULTS AND DISCUSSION

We have developed an authentication system with three layer security using the algorithms of machine learning and some image processing concepts. Below are the snapshots of the output:

Fig 6: Login Page

Fig 7: Registration Page

Fig 8: Virtual Keyboard for safe PIN entry

VI. CONCLUSION

This new system for authentication called “Password Authentication Provided by Three Layer Security Using Machine Learning”, has been developed with the help of laptop camera or a small web cam. Currently this system is developed for nine digit based PIN entry. It can further be updated with different combination based PIN entry, but the disadvantage of

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86122

increasing more combinations would be time complexity. In order to overcome that a very effective system with web cam has to be used so that it can detect the eye blinks at a faster rate.

VII. FUTURE SCOPE

While our system provides promising results it can still be upgraded to the best possible way. This system can be implemented with iris scanner function which provides very high security comparatively. We can also include gaze patterns with the help of a strong web cam to overcome the time complexity problem. A separate research has to be conducted to develop strong algorithms which help in making the present system much promising.

REFERENCES

[1]. Aureliene Geron, "Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems", March 2017
[2]. Aaron Courville, Ian Goodfellow, and Yoshua Bengio, "Deep Learning",2015.
[3]. Gonzalez and Woods, "Digital Image Processing ".
[4]. Anil Kumar Jain and Stan Z.Li, "Handbook of Face Recognition",2005.
[5]. Top Cyber Threats for 2016; integrity attack on financial sector likely.http://www.carriermanagement.com/news/2015/11/30/148345.htm.
[6]. W. Ashford. Info security Europe 2010: Data integrity attacks to become more common, say experts. http://www.computerweekly.com/news/1280092630/Infosecurity-Europe-2010- Data-integrity-attacks-tobecome-more-common-say-experts.
[7]. Eye blink with OpenCV, Python and dlib by Adrian Rosebrock on April 24, 2017. https://www.pyimagesearch.com/2017/04/24/eye-blink-detection-opencv-python-dlib/