PASSWORD AUTHENTIFICATION THROUGH REAL-TIME EYEBLINKING

[1]**Ramesh B E**
Asso.Prof, Dept CS&E, SJMIT,Chitradurga,India
be.ramesh@gmail.com

[2] **Shruthi M** K
Asso.Prof, Dept CS&E, SJMIT,Chitradurga,India
mksshruthi@gmail.com

[3] **Sneha** U
Dept CS&E, SJMIT,Chitradurga India
sneha.u2223@gmail.com

[4]**Vinith J**
Dept CS&E, SJMIT,Chitradurga,India
vinujavli3@gmail.com

[5] **Thilak Bannenar H E**
Dept CS&E, SJMIT,Chitradurga,India
thilakhe6@gmail.com

[6] **Haleema Misbah Noorain**
Dept CS&E, SJMIT,Chitradurga,India
haleemamisbahnoorain@gmail.com

***Abstract*—There are several systems that employ unique identification digits for user verification and security. PIN-based password verification requires users to type in a physical PIN, thereby making it easy for hackers to figure out or guess the password. using shoulders to surf or thermal energy tracking. On the other hand, PIN input techniques do not leave any physical traces and offer a more secure password entry option. PIN authentication using passive eye movements. Eye blinks-based validation is the process of identifying an individual's eye blinks in a sequence of frame photographs or by producing a PIN. During this research, we combine recognition of faces, eye blink-based PIN input, OTP (One Time Password), and real-time application to counter threats from thermal tracking and surfing with the shoulders.**

Keywords—user verification,OTP,PIN,password,eye, blink,shoulder.

I. INTRODUCTION

One of the general terminal's security criteria. People must deal with authentication processes every day thus authentication solutions must be simple, quick, and secure. use passwords or other traditional knowledge-based methods to authenticate oneself. However, these methods are not secure because they are watched by unscrupulous observers who use surveillance methods like shoulder-surfing (observing a user while they type a password on a keyboard) to record user authentication information. Additionally, there are security issues brought on by subpar user and system interactions. In order to safeguard PIN numbers, the researchers devised a three-layered security architecture. Users input the password by blinking their eyes at the relevant symbols in the proper order, making them immune to shoulder surfing. The purpose of this essay is to discuss methods or responses for addressing eye blink in security systems.

Attacks on ATMs by fraudsters have been more frequent in 2016 compared to 2015, according to European ATM Security. This is because there aren't enough personal identification numbers (PINs), which are essential for verification in a variety of contexts, including managing cash at ATMs, approving financial transactions online, unlocking mobile devices, and unlocking doors. Password attacks like thermal tracking and shoulder surfing may also be used against PIN entering.

II. SPECIFICATION OF THE ALGORITHM

A. HARR CASCADE CLASSIFIER

Paul Viola and Michael Jones proposed an effective object identification method that makes use of Haar-based cascade classifiers with features in their study "Rapid Recognition of Objects using a Boosted Cascade of Simple Features" from 2001. This machine learning-based method learns a cascade value from a huge number of pictures, both positive and negative. Then, using it, object detection in additional photos is carried out.

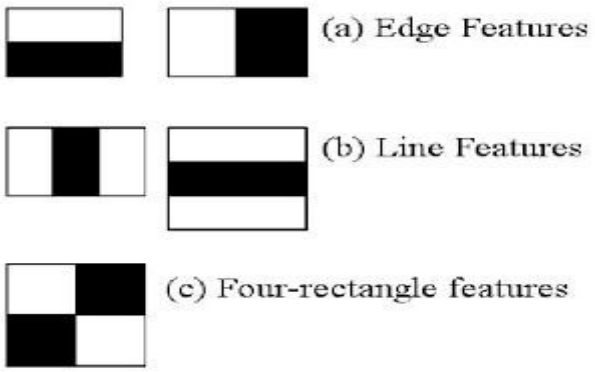

Figure 1:Different Features

In this case, face detection will be employed. The method initially needs a large number of positive photographs (pictures

with faces) and bad pictures (representations without faces) to train the classifier. Then, we must infer characteristics from it. The figure underneath shows all of the Haar features that are used for this. In every way, they mimic our multilayer kernel. Each character is represented by a single value that can be determined by subtracting the sum of the pixels under the white and black rectangles from the total number of pixels below the white rectangle. Now, many features are computed with each kernel in a variety of places and sizes. (Just try to imagine how much computation is needed. Even in a 24x24 timeframe, 160000+ features can be generated. For every aspect of computation, the number of pixels under the white and black squares must be determined. To remedy this, the integrated image was developed. No matter what size the photograph is, it simplifies the computations for each pixel in the image to a straightforward four-pixel procedure. It makes everything faster.

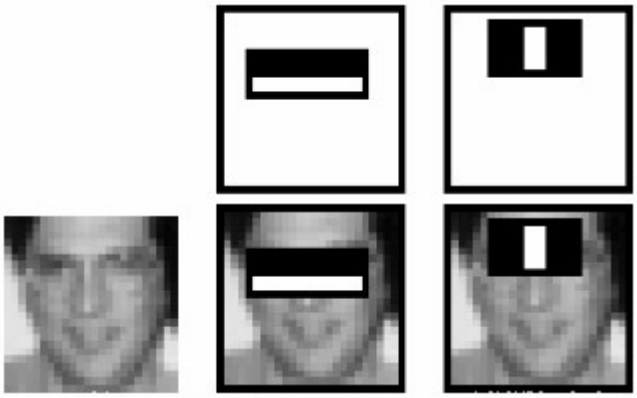

Figure 2: Focusing Features

We use each and every characteristic to accomplish this on every practice image. To classify the features as either favorable or detrimental, it establishes an appropriate threshold based on each excellence. There will surely be errors or misclassifications. We select the traits that, with the least degree of error, classify images of people and goods that do not include features. (The process is not that simple. Each picture starts off with the same weight. Following each categorizing, the relative importance of the wrong organized photos rises. The same process is then carried out. New rate of error were calculated. computed. as well as new weights. Until the proper accuracy, error rate, or number of features is identified, the process is repeated.

The ultimate predictor is a weighted mean among these poor scorers. It is called weak because, when used in conjunction with other classifiers, it may classify a picture even if it is unable to do it on its own. According to the study, even 200 traits may produce 95% accurate detection. They final arrangement offered roughly six thousand features. Instead of allowing 160000+ features, set a cap of 6,000 features. That represents a sizable gain. So you just take a picture. Consider every 24x24 window. Think of adding 6000 features to it. Make sure the thing isn't a face. It seems a little inefficient and time-consuming. Undoubtedly, it is. The writers provide a sound solution to the issue. The majority of a photograph's depiction sin not a face. Being able to quickly assess whether a window is a face region is therefore preferable. If not, discard it right away and don't process it again. Instead, focus on potential locations for faces. We can check additional possible face locations by doing this. In order to contend address this, they developed a concept of a sequence of classifiers. Instead of being applied all at once to a window, the 6000 features are separated across several classifier steps. There are frequently many fewer features in the first few phases. If an opening fails the first test, discard it. It does not take into consideration the extra features. If it triumphs, use the following category of characteristics and continuing with the process. The window that successfully completes all phases is the face area.

There were a total of one ten, twenty-five, and fifty distinct characteristics in each of the initial four phases of the authors' detector, which is which had 6k+ characteristics and 38 divisions. The leading two traits found in the Ad boost system were merely picked to symbolize each of the characteristics in the aforementioned image. According to the creators, based on a little over 6,000 traits, each channel-window analyses 10 qualities on mean.

So far, this provides a clear, concise explanation of how Viola-Jones facial recognition works. See the journal or the sources identified in the further reading section for greater information.

CNN:

The design stage is most important in all of it since we are constructing an CNN whereby we will enter our features to train our model then trial them with the actual elements. We amalgamated a number of distinctive capabilities, which we shall go through by themselves, to produce CNN.

Sequential() - When building an ordered model, each of the layers are simply added the other after the other as we move from the layer that contains inputs to the output layer. It applies the batch standardization operation to inputs to the following layer in order to show the data we supply on an appropriate scale, say between zero and one, compared to having it distributed all throughout the whole layer.

model.add(Conv2D())- The particular instance in problem-solving executes utilizing the convolution methodology laid out at the initial stage of the current element, model. Add(Conv2D()). It's a 2D neuronal layer. Per to the palm-written Kera's, "This stratum supplies a kernel for convolution that can be combined with its layer's output for generating an integer number with outputs." Our function of activation here relates to the rectangular unit of measurement (REL), and a kernel is 3x3 in dimension.

model.add(BatchNormalization())- upon order to display what we input over an agreed-upon production, such 0 to 1, without being spread all through the whole layer, template. Add(BatchNormalization()) performs the batch standardization approach on signals to the being successful layer.

model.add (MaxPooling2D())-onto the structure of the model-The above technique will involve the information aggregating manipulate, as indicated near the very beginning of the sentence. We used a 2 by 2 windows sharing with 2 x 2 sweeps in this framework..

model.add(Dropout()) - Drop out is an algorithm that, already noted, avoids the overfitting by forgetting selective neurons while development and "pouring these out" at arbitrary. model. Add(Dropout ()) is an approach that uses the above method.

model.add(Flatten()) - strictly reduces the supplied data into ND back 1D; the resultant batch dimension stays unaffected.

model.add(Dense()) - Heavy provides a certain formula: model. Add(Dense()) product is the same as dot (input, kernel), whereby foundation is a coat-generated coefficients tensor and stimulation is the part-wise activation function that is given as the function's activation factor. It is, in simple terms, the final warning knell which links the traits learnt during layer learning to the label. This part of the process is in responsible for producing the final label on the test imagery that will be analyzed

B. MODULES

CNN FOR FACE RECOGNITION

Let's look at how effectively people understand faces first. The understanding of appearances is pretty challenging because so many distinct and huge brain networks play a part in absorbing emotions. In neurological studies, the fusiform gyrus, which has been proven to cause prosopagnosia when damaged (particularly when an inflammation affects both lobes), may be quite active. People learn to recognize their faces at a young age and can distinguish one individual from another virtually right away.

Humans tend to pay close attention to the eyes, cheekbones, nose, lips, brows, skin texture, and skin color. Our brain simultaneously examines the full face and can identify a person even from only a small section of it. By comparing the final image with its own assessing pattern, the central nervous system detects the spatial mismatch.

The initial stage is for the facial analysis algorithm to locate then display the human visage on the snapshot. A number of techniques, including those for comparing dimensions and skin tone, choosing contours in the image and comparing them to those of faces, and choosing symmetries using neural networks, can be used by the programme to do this. The Viola-Jones approach, which may be applied in real-time, is most efficient. With it, the system can identify faces despite rotations of 30 degrees.

The method is based on the indications of Haar, a set of irregularly shaped triangular black and white masks. Preceding establishing the variance between the two values, the technique includes the value of brightness from each pixel in the photo that is concealed by the black and white portions of the mask. The masks are superimposed over different areas of the image. The machine learning method tracks the human face in the picture, contrasts the results with the information, and maintains track of it to determine the ideal angle and image quality. For this, motion vector prediction techniques or correlate technologies are used.

The algorithm runs identification of faces off the best captures it has chosen, then compares the findings to the existing data collection. The programme finds the exact points on the person's face that constitute up the various characteristics, much like a portrait artist does. 100 of these points are normally awarded by the programme. the application of algorithms or algorithms for correlation.

One of the many crucial metrics for software that recognizes faces is the space between both eyes, the width of the nasal passages, the diameter of the nasal passages, the shape and height of the jowls, the width at the chin, and hair height of the crown of the head, besides other characteristics. When the conditions match, the data gathered undergoes comparison with what is in the database, and the person is located.

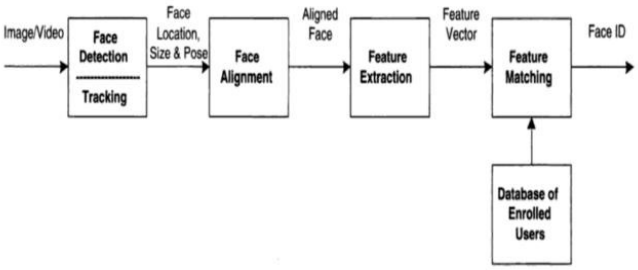

Figure 3 : Face Recognition Processing Flow

C. PASSWORD GENERATION USING EYEBLINK

In our project, the digital keyboard is shown on the screen as the second stage of verification. Whenever someone flashes their eyes, one pointer is going to continue shifting across their computer keyboard as the PIN number is generated using the sequence of numbers that were collected. The webcam is being used to record eye movements. OpenCV is being used to identify eye blinks.

Utilizing image bookmarking and OpenCV as we are going to build on this data to develop a computer graphics program that is able to recognize and compute streaming video failures.

We will make use of an indicator known as eye factor ratio (EAR) to construct the more exact detectors.

Unlike conventional computer animation methods, which often combine:

1. Localizing the eyes.
2. Thresholding to locate the eye whites.
3. Observe whether the "white" area of the eyes vanishes for a while (signifying a blink).
4. The eye aspect ratio, which is based on the ratio of the distance among the prominent features of the eyes, is a far more beautiful alternative.

D. GENERATION AND VERIFICATION OF OTP

This is the third degree of protection, and to create the one-time password (OTP) and deliver it to users through email or mobile phone and safeguard their accounts, random integers are used.

III. IMPLEMENTATION

Facial tangibility: Since the surface of the face has symmetry, we employ a symmetry-based strategy. We discovered that using a grayscale sample version is enough.

In the squeezed image, the uniformity value is first figured out, and then it is calculated across the pixel the columns. The symmetry value for a pixel column is provided by S(x) = [abs I ((x, y-w)-(x, y+w))] if the picture is expressed as I(x, y).For X € [k, size-k], S(x) is calculated where k is the greatest distance from the pixel-column that symmetry is assessed, and x size is the picture width. The face's centroid is the x who is equivalent to the minimal measurement of S(x).

Eye monitoring: For the purpose of monitoring an eye, they search to identify the darkest image within the anticipated area. We ensure that none of the geometrical requirements are broken in order to recover from tracking mistakes. If so, we relocate the eyeballs in the following frame. We first center it at the darkest pixel and then use a gradient descent to get the closest

minimum to figure out the most ideal match for the human retina template.

To prevent infrared tracking and shoulder surf attacks, I will provide a three-layer stage security architecture. Our technology has three layers: face reorganization, eye-blink verification, and one-time password. We will apply our security architecture to prevent shoulder surfing and thermal tracking threats by merging all of these layers. Because there is no physical input of passwords in our system, we are completely protected against shoulder surfing and thermal tracking attacks. We use the Deep Learning method for the first degree of security, and Vision for the supplementary layer.

Based on the disparities across the two pictures, you get ° ng for the backdrop locations of the eye. We emphasize the skull cleaning method in order to differentiate them from headaches. Regardless of the actual eyes, an outline of an eye is produced for each structure using the "Between the Eyes" template. The location of the pupil "Between-the-Eyes" and their geometric relationship to the preceding location are thought to constitute the foundation for the eyes.

IV. SYSTEM ARCHITECTURE

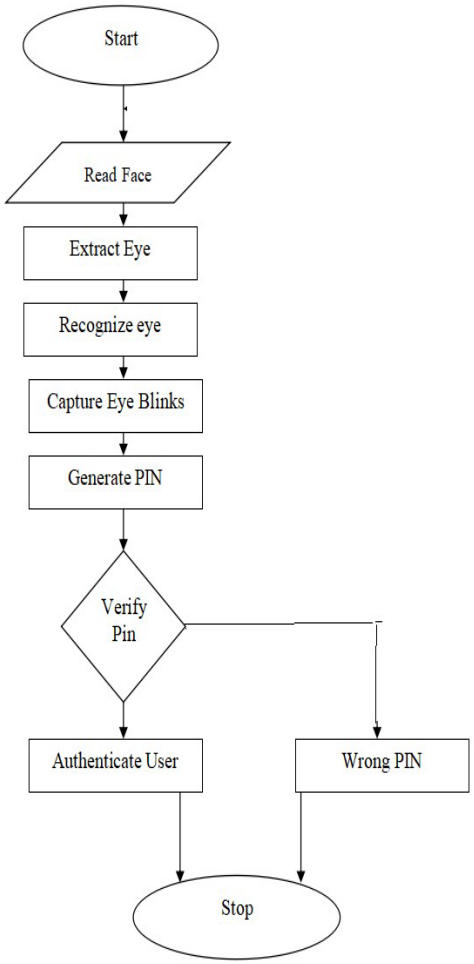

Figure 4: System Architecture

V. DATA FLOW DIAGRAM

The DFD is additionally known as a bubble chart. It is a simple pictorial framework that could be employed to represent an organization. Different processes are dispersed on this data, and as a result, the structure produces the output data.

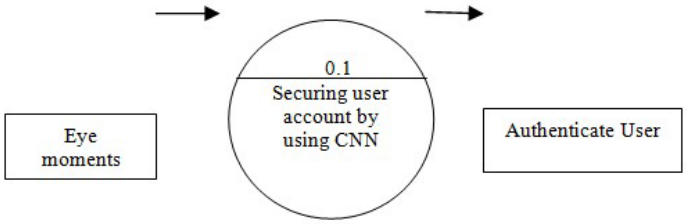

Figure 5.1

Users' eye movements are being used as input. The technology will protect user account information against shoulder-to-shoulder hurts using conventional neural networks.

Level: 1

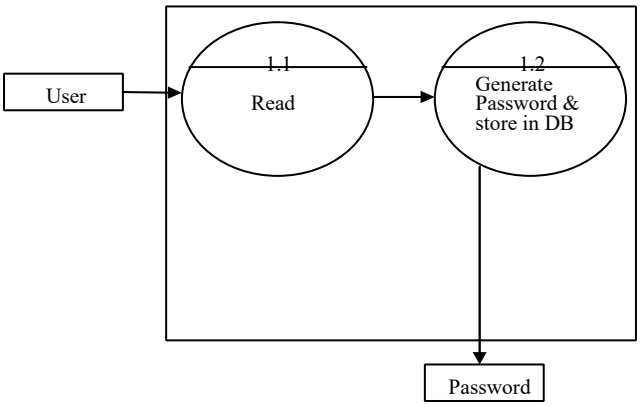

Figure: 5.2

Level: 2

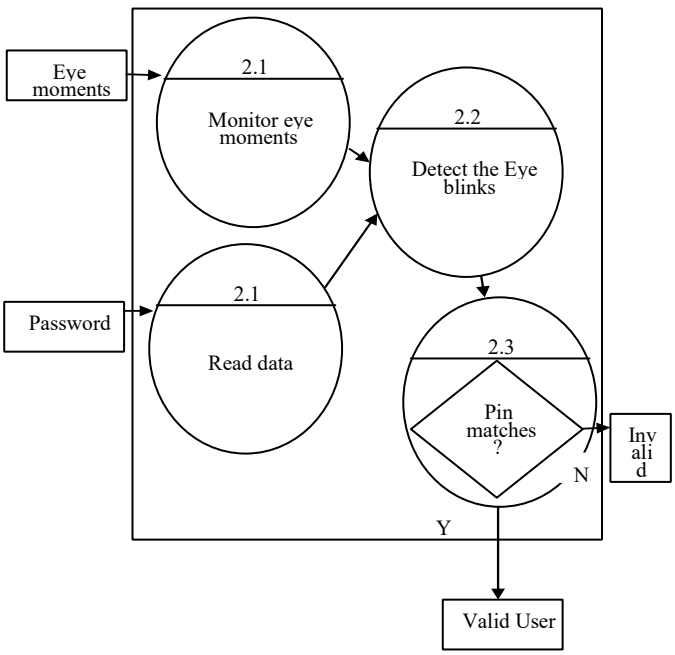

Figure: 5.3

CONCLUSION

A novel application for eyelid blink-based PIN identification has been invented that uses a smart camera-based eye-blinking technology. The system may be expanded to allow for character and digit combination credential stepping into and was successfully tested with a nine-digit keypad. The accuracy of the detected pins will be dependent on the user's eye blink equilibrium, therefore this must be taken into attention. At the moment, real-time eye blinks and eye center calculations and recording are finished before the PIN recognition is done.

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. (Available: http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue4/Version2/B017420915.pdf)

[2] J. Weaver, K. Mock and B. Hoanca a, "Gaze-Based Password Authentication through Automatic Clustering of Gaze Points," Proc. 2011 IEEE Conf. on Systems, Man and Cybernetics, Oct. 2011. (DOI: 10.1109/ICSMC.2011.6084072)

[3] "ATM Fraud, ATM Black Box Attacks Spread Across Europe", European ATM Security Team (E.A.S.T.), online, posted 11 April 2017. (Available: https://www.europeanatm-security.eu/tag/atmfraud/)

[4] K. Mowery, S. Meiklejohn and S. Savage, "Heat of the Moment: Characterizing the Efficacy of Thermal CameraBased Attacks," WOOT '11, pp. 1-8, August 2011. (Available: https://cseweb.ucsd.edu/~kmowery/papers/thermal.pdf)

[5] M. Mehrübeoglu, H. T. Bui and L. McLauchlan, "Real-time iris tracking with a smart camera," Proc. SPIE 7871, 787104, 2011. (DOI:10.1117/12.872668)

[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. (DOI: 10.1109/AIPR.2011.6176373)

[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, id. 843705, 2012. (DOI: 10.1117/12.922875)

[8] Smart Cameras for Embedded Machine Vision, (product information) National Instruments (Available: http://www.ni.com/pdf/products/us/cat_ni_1742.pdf)