IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

EYE BLINKING FOR PASSWORD AUTHENTICATION

[1] SARAVANAKUMAR [2] DEEPAKRAJ N [3] CHANDANA V [4] RAKSHITHA E S [5] YASHASWINI S

[1] Assistant Professor, Computer Science, Dayananda Sagar Academy of Tech & Mgt, Karnataka, India [2] B.E. 4th year, Computer Science, Dayananda Sagar Academy of Tech & Mgt, Karnataka, India [3] B.E. 4th year, Computer Science, Dayananda Sagar Academy of Tech & Mgt, Karnataka, India [4] B.E. 4th year, Computer Science, Dayananda Sagar Academy of Tech & Mgt, Karnataka, India [5] B.E. 4th year, Computer Science, Dayananda Sagar Academy of Tech & Mgt, Karnataka, India

Abstract— This paper focuses on entry of PIN exploitation blinking method.

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. Eye blinks-based authentication refers to finding the attention blinks across sequent image frames, and generating the PIN. 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 personaldevices ,event centers, shopping malls, Medical centers, schools/collages and opening. doors.

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 ourselves in 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 a group 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.

one among the safety necessities for general terminal authentication system is to be simple, quick and secure as folks face authentication mechanisms on a daily basis and should authenticate themselves victimization standard knowledge-based approaches like passwords. however these techniques square measure not safe as a result of they're viewed by malicious observers World Health Organization use police investigation techniques like shoulder-surfing (observation user whereas writing the parole through the keyboard) to capture user authentication knowledge. Also, there are security issues thanks to poor interactions between systems and users. As a result, the researchers planned a three- layered security framework to secure PIN numbers, where users will enter the parole by blinking the attention at the suitable symbols within the acceptable order and so the user is invulnerable to shoulder surfboarding. Eye blinking may be a natural interaction methodology and security systems supported nictitation tracking offer a promising resolution to the system security and usability. The aim of this paper is to review techniques or solutions to coping with nictitation in security systems. The utilization of non-public identification numbers (PINs) may be a common user authentication methodology for several applications, such a cash management in automatic teller machine machines (ATMs), approving electronic transactions, unlocking personal devices, and gap doors. Authentication is always a challenge even once victimization PIN authentication, such as in monetary systems and entryway management. to European ATM Security, fraud attacks on ATM inflated by twenty sixth in 2016 compared to it of 2015. the very fact that associate authorized user should enter the code in open or public places make PIN entry at risk of parole attacks, such as shoulder surfboarding additionally as thermal trailing.

ALGORITHM SPECIFICATION

HAAR CASCADE CLASSIFIER:

The acquisition of an object victimization the HAAR-based platform is an effective technique of object discovery projected by Paul Viola and Michael Jones in their paper, "Recent Acquisitions Using Enlarged Cascade. It is a machine learning technique where Cascade's work is trained from several positive and negative pictures. Then it's wont to notice objects in different images .Initially, the algorithm needs many good pictures (face pictures) and negative images (images without faces) to train the coed. At that time we'd like to extract options from it. During this case, exploitation the HAAR options shown within the image below. Now, all attainable sizes and locations of every kernel area unit used to calculate multiple options. To calculate every component, we need to notice the total of pixels below the white and black squares. To resolve this, they introduced a crucial image. Even

though your image is giant, it limits the component count provided to practicality that involves simply four pixels. But among all the options we've got listed,several of them don't work.

The primary feature elect looks to concentrate on the properties of the attention region that's usually darker than the nose and tire region. But among of these options we have a tendency to calculated, most of them area unit digressive. For instance, contemplate the image below. The highest row shows 2 sensible options. The primary feature selected looks to concentrate on the property that the region of the eyes is commonly darker than the region of the nose and cheeks. The second feature elect depends on the property that the eyes area unit darker than the bridge of the nose. However an equivalent windows applied to cheeks or the other place is digressive. So however will we choose the simplest options out of 160000+ features? It is achieved by Adaboost. In this case, we have a tendency to apply every component to any or all coaching pictures. At each stage, you get a extremely sensible edge that may distinguish the face from sensible and unhealthy. we have a tendency to choose the options with a tiny low error rate, which suggests they're the options that distinguish the faces from the non- face pictures. (The method isn't as simple as this. every image is given an equivalent weight at the beginning. when every split, the illegals of the sculpture increase. The process continues till the accuracy or error rate is reached or the amount of options is reached).The final classifier may be a weighted total of those weak learners. it's known as weak as a result of it alone won't distinguish the image, but in association with others it creates a powerful bonding part. The paper states that even two hundred options give ninety fifth accuracy. (Consider a reduction from 160000 options to 6000 options. The authors have an honest answer for that. For an image r, most of the image is extent. thus it is a sensible idea to possess a straightforward thanks to confirm a window isn't a surface. If not, get obviate it by firing one, and never have a go at it once more. Instead, concentrate on regions wherever there is also faces. This way, we pay a great deal of your time viewing potential regions of the face. They bestowed this idea within the Cascade of Classifiers. Instead of exploitation all 6000 objects in an exceedingly window, the options area unit organized into completely different categories of learners and worked individually. (Generally the primary few paragraphs can contain very few features).If a window fails within the initial section, discard it. If it passes, use the second part of the symptoms and continue the method. the best window of all categories is that the face space.The authors' detector had 6000+ features with thirty eight stages with one, 10, 25, twenty five and fifty options in the first 5 stages. (The 2 options within the on top of image area unit actually obtained because the best 2 options from Adaboost). According to the authors, on the average ten options out of 6000+ are evaluated per sub-window. thus this is often a straightforward intuitive explanation of however Viola-Jones face detection works. Read the paper for a lot of details or cross-check the references within the Additional Resources Section.

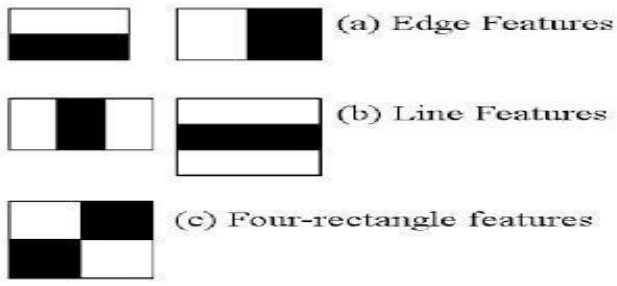


FIG: Different Features

CNN MODEL

This step is that the most significant a part of the whole method as we style the CNN through that we'll pass our options to train the model and eventually check it mistreatment the check features. we've used a mixture of many completely different functions to construct CNN that we'll discuss one by one.

1. **Sequential()** - A sequent model is simply a linear stack of layers that is golf stroke layers on high of every other as we have a tendency to progress from the input layer to the output layer.

2. **model.add(Conv2D())** - this is often a second Convolutional layer that performs the convolution operation as described at the start of this post. To quote Keras Documentation "This layer creates a convolution kernel that's convolved with the layer input to provide a tensor of outputs." Here we have a using a 3x3 kernel size and corrected long measure (ReLU) as our activation perform.

3. **model.add(BatchNormalization())** - It performs the batch social control operation on inputs to the next layer so we've our inputs in an exceedingly fixed scale say zero to one rather than being scattered everywhere the place.

4. **model.add(MaxPooling2D())** - This perform performs the pooling operation on the info as
explained at the start of the post. we have a tendency to ar taking a pooling window of 2x2 with 2x2 strides during this model

5. **model.add(Dropout())** - As explained higher than Dropout may be a technique wherever willy-nilly elect neurons ar unheeded throughout the coaching. They are "dropped out" willy-nilly. This reduces overfitting.

6. **model.add(Flatten())** - This simply flattens the input from ND to 1D and doesn't have an effect on the batch size.

7. **model.add(Dense())** - in line with Keras Documentation, Dense implements the operation: output = activation(dot(input, kernel)where activation is that the element-wise activation perform passed as
the activation argument, kernel may be a weights matrix created by the layer. In straightforward words, it's the ultimate nail within the coffin that uses the options learned using the layers and maps it to the label.
During testing, this layer is chargeable for making the ultimate label for the image being processed.

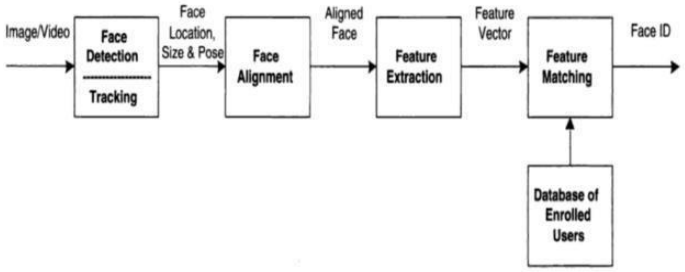
FACE RECOGNIZATION

Let's look 1st on however human do acknowledge the faces. Face perceptions ar terribly advanced because the recognition of facial expressions involves intensive and various areas in the brain. Brain imaging studies generally show an excellent deal of activity in a locality of the lobe referred to as the pointed complex body part, a locality conjointly best-known to cause prosopagnosia once broken (particularly once damage happens on each sides). folks learn to acknowledge faces from birth and nearly at the age of 4 months will clearly distinguish one person from another. The main factor that someone pays attention to is that the eyes, cheekbones, nose, mouth, and eyebrows, still because the texture and color of the skin. At an equivalent time, our brain processes the face as an entire and is ready to spot a person even by half the face. The brain compares the resulting image with the inner mensuration pattern and receives the point distinction.

First, the face recognition system has to notice the face in the image and highlight this space. For this, the computer code can use a range of algorithms: for instance, determinant the similarity of proportions and color, the choice of contours within the image and

their comparison with the contours of faces, the choice of symmetries mistreatment neural networks.The foremost effective is that the Viola Jones method, which might be employed in real time. With it, the system acknowledges faces even once revolved thirty degrees. The method relies on the signs of HAAR, that ar a group of black and white rectangular masks of various shapes. The masks ar superimposed on completely different components of the image, and therefore the rule adds the brightness of all the pixels of the image that ar underneath the black and white parts of the mask and so calculates the distinction between these values. Next, the system compares the results with the accumulated information and, having determined the face within the image, continues to trace it to select the optimum angle and image quality. For this purpose, motion vector prediction algorithms or correlation algorithms are used.

Having chosen the foremost roaring photos, the system proceeds to face recognition and its comparison with the existing base. It works consistent with an equivalent principles as the creative person paints portraits — the program finds the reference points on the person's face that conjure the individual options. As a rule, the program allocates regarding 100 such points. The most vital measurements for face recognition programs ar the space between the eyes, the breadth of the nostrils, the length of the nose, the peak and form of the cheekbones, thebreadth of the chin, the peak of the forehead and different parameters. After that, the obtained data ar compared with those accessible withinthe information base, and, if the parameters coincide, the person is known.



EYE BLINK GENERATION

This is the second layer authentication in our project we tend to area unit displaying the digital keyboard on the screen. One indicator can keep getting the digital numeric keyboard once user blinks eye system can generate the number from collect the sequence of numbers that user blinks eye. we tend to area unit mistreatment the web camera to observe eye moments. we tend to area unit mistreatment OpenCV to detects nictitation. We will depend on this information and develop a laptop visualization app which will sight and calculate video stream crashes mistreatment face bookmarks and OpenCV. To build our a lot of correctdetector, we are going to be employing a metric called eye issue magnitude relation (EAR).

Unlike ancient laptop animation techniques that involve some combination of:

1. Eye localization.

2. Thresholding to search out the whites of the eyes. deciding if the "white" region of the eyes disappears for aamount of your time (indicating a blink).

3. the attention ratio is instead a far a lot of elegant solution that involves a awfully straightforward calculation primarily based on the magnitude relation of distances between facial landmarks of the eyes.

OTP GENERATION AND VERIFICATION

This is the third level of security we are using the random numbers to generate the otp and send to users email/ mobile number using the otp we can secure our accounts.

EXISTING SYSTEM

In current state of affairs the ways in which of returning into passwords square measure

through hand, in terms of pin and passcodes, which as compared to latest technology aren't enough safe. This statement thought of to be correct as a results of we've to suppose of that wherever current technology is heading and wherever square measure we've a bent to in this trend. so on influence completely totally different systems we've a bent to as well should have enough sources for a similar throughout this technological era as like providing safety to crucial workstations with certain system containing a durable identification. The use of non-public identification numbers (PINs) may be a common user authentication methodology for many applications, like cash management in ATM machines (ATMs), approving electronic transactions, unlocking personal devices, and gap doors. unflawed

identity authentication remains a challenge even once PIN authentication is employed, like in monetary systems logic gate access management. in step with European ATM Security, fraud attacks on ATMs increased by twenty sixth in 2016 compared to 2015.

PROPOSED SYSTEM

We are a unit getting to propose the three-layer security theme to avoid the shoulder aquatics and thermal following attacks. Our system contains the 3 layers that area unit one. Face reorganization, 2. Eye- blink verification, and 3. OTP by combining all this layers we tend to area unit getting to implement our secure framework to avoid shoulder aquatics and thermal following attacks. In our frame works there is no physical entry of countersign therefore we tend to area unit utterly avoiding the shoulder aquatics and thermal following attacks. For the primary layer security we tend to area unitvictimization Deep Learning formula., for the second layer we tend to area unit victimization OpenCV. The strategies for coming into passwords are often created safe enough victimization latest strategies like eye following. It means that create use of your eyes which can not leave prints like when we enter positive identification by hands, which may be retrieved through colloid, thus there's no purpose of safe entryof password. So, the attention following system are often used for safer options that got several strategies in it, here we decide is that the method like blinking of eye for positive identification authentication, which will not leave any prints behind.

RELATED WORK

There are various authentication mechanisms that have been implemented in the real world so far. Some of the methods /algorithms used earlier are described in further subsections of this chapter. The assumptions are, the user has to input each digit in the pin separately. For instance, if the input PIN is of length 4, the user is prompted to blink an eye once at the specific digit in 4 different screens. That is, for each PIN digit in 4 different keypad screens. The study of existing methodologies that are based on Password/PIN authorization is summarized. A paper on Advanced Safe PIN-Entry against Human Shoulder-Surfing follows black and white colored mechanism where a numeric keypad is colored at odd in each round. Any user can enter PIN by pressing a specific color. This proposed model is found vulnerable to shoulder surfing attacks and hence does not help in secured authentication.

The paper Gaze-Based Password Authentication through Automatic Clustering of Gaze Points follows gazing technique in order to giveinput.

The user's PIN is authenticated by gaze points. In this approach, the user looks at the appropriate symbol/digit and gaze points are automatically clustered by the algorithm to determine the selected digit. This approach uses a simple clustering technique to cluster the gaze points, but the results of clustering accuracy is found to be less than 83%. The paper Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks demonstrates the use of thermal cameras in recovering PIN typed on keypad.

The password can be recovered easily using thermal sensors within less than a minute after PIN entry. Although there were many preventive measures adopted earlier, it does not provide more secure authentication for user's making transactions or any other operations in an security systems. Hence, few drawbacks of each model were collected and our paper is found to overcome shoulder surfing as well as thermal attack to greater extent with more additional secured layers. Our proposed system works well having a series of authentication systems starting from recognition of the user's face as first layer, detecting the eye blink and invulnerable PIN entry till generating OTP and sending it to account holder for additional security purpose.

ARCHITECTURE MODEL

The diagram shown below showcases the exact working of the password authentication model of the proposed system.

The execution initially starts with recognizing the face.

The detection of blinking and the analysis of blink duration are based solely on observation of the correlation scores generated by the tracking at the previous step using the online template of the user's eye. As the user's eye closes during the process of a blink, its similarity to the open eye template decreases. Likewise, it regains its similarity to the template as the blink ends and the user's eye becomes fully open again. This decrease and increase in similarity correspond directly to the correlation scores returned by the template matching procedure.

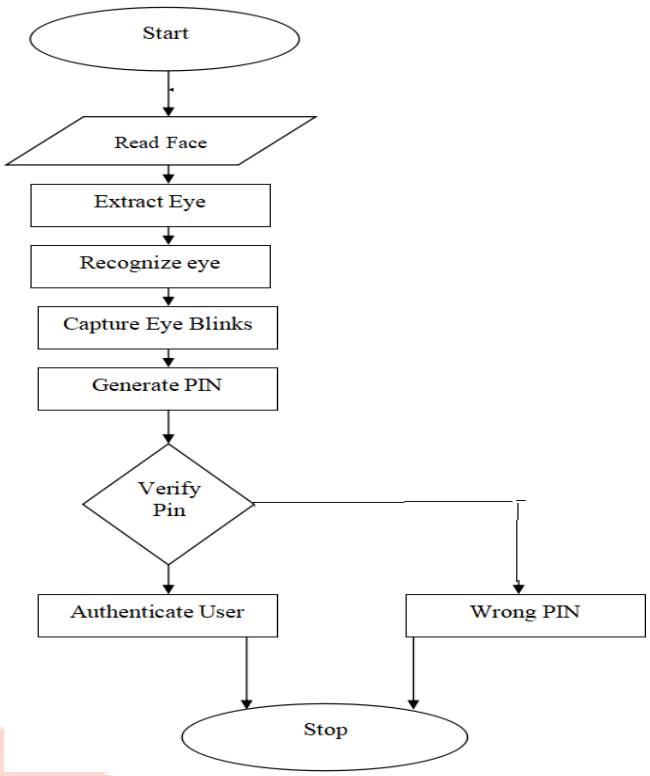
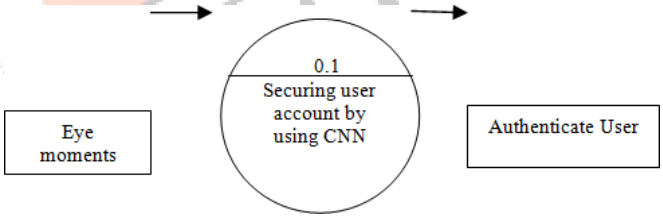


FIG: System Architecture

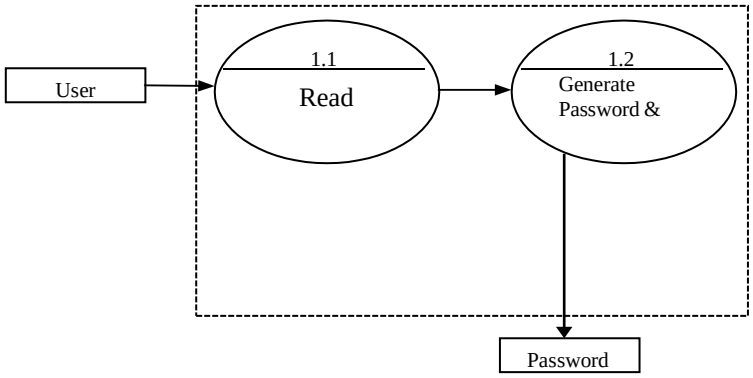
DATAFLOW DIAGRAM

The DFD is also referred to as bubble chart.It is an easy graphical formalism that can be used to represent a system,varied process distributed on this data,and therefore the output data is generated by this system.

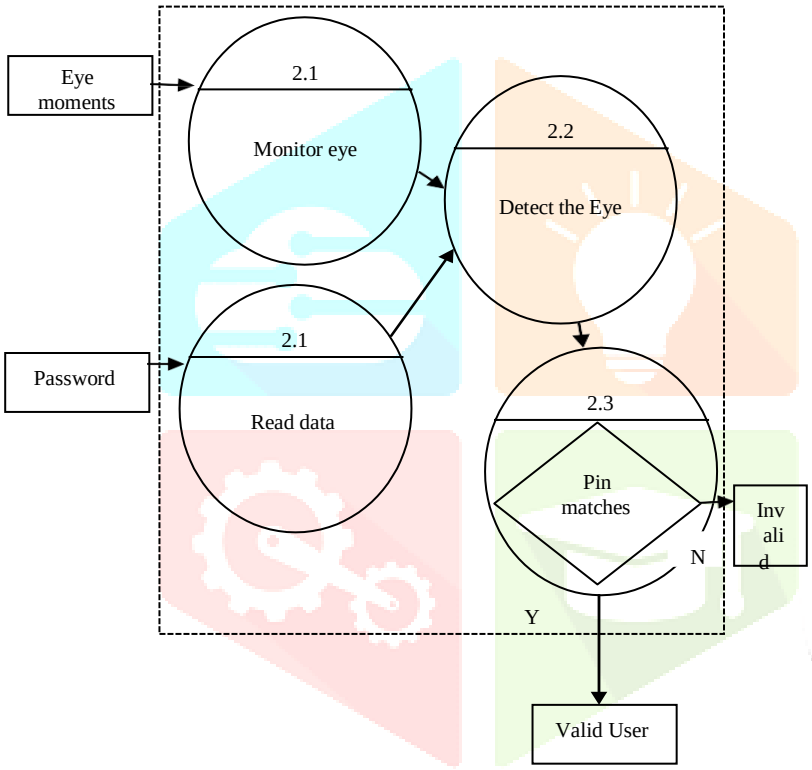


We are using users eye moments as input. System will use the conventional neural network to secure user account informationfrom shoulder surfing attacks.

Level:1:



Level:2:



LITERATURE SURVEY

TOPIC: Eye tracking recognition-based graphical authentication AUTHORS: M. Martin, T. Marija and A. Sime, PUBLICATION: 7th International Conference on Application of Information and Communication Technologies, Baku, 2013, PP. 1-5. doe: 10.1109/ICAICT.2013.6722632.

The shift towards including human factors as part of system design has a direct impact on the security of the system. The users' misunderstanding of how a secure mechanism works usually results in security failures.

People encounter security mechanisms daily, most often required to authenticate themselves using knowledge-based schemes such as passwords, the most common and prevalent type of authentication mechanisms plagued with security and usability problems. As technical solutions have not resolved the usability of passwords many passwords used in practice are either weak and usable or secure and unusable. Hence, in recent years graphical passwords have been proposed as a potential solution due to their improved usability features and the superior human ability to recognize and remember images. TOPIC: SAFE: Secure authentication with Face and Eyes AUTHORS:

A. Boehm et al. PUBLICATION: 2013 International Conference on Privacy and Security in Mobile Systems (PRISMS), Atlantic City, NJ, 2013, PP. 1-8, doi: 10.1109/PRISMS.2013.6927175. Face authentication is commonly offered as an alternative to passwords for device unlock. However, available face authentication systems are vulnerable to simple spoofing attacks. Author demonstrated the impact of image quality on spoofing, using low representative of those commonly posted online. resolution photo. To defend against these vulnerabilities, they propose a face authentication system that includes a secrecy challenge. SAFE (Secure Authentication with Face and Eyes 1), an improved face authentication method was proposed that uses a commodity gaze tracker to input a secret. During authentication, the user must not only show her face but also gaze at a secret icon that moves across the screen. Using a novel method for estimating the noise level in the gaze tracking data, SAFE adapts the system's parameters to enable secure, hands-free authentication. TOPIC: Using machine learning to detect events in eye-tracking data. Behavior Research Methods AUTHORS: Zemblys, Raimondas & Niehorster, Diederick & Komogortsev, Oleg & Holmqvist, Kenneth. PUBLICATION: (2017) 50. 10.3758/s13428-017- 0860-3. Event detection is a challenging stage in eye movement data analysis. A major drawback of current event detection methods is that parameters have to be adjusted based on eye movement data quality. In this work author shown that a fully automated classification of raw gaze samples as belonging to fixations, saccades, or other coulometer events can be achieved using a machine learning approach. Any already manually or algorithmically detected events can used to train a classifier to produce similar classification of other data without the need for a user to set parameters. Random forest machine-learning technique used for the detection of fixations, saccades, and post- saccadic oscillations (PSOs).In an effort to show practical utility of the proposed method to the applications that employ eye movement classification algorithms, provide an example where the method is employed in an eye movement-driven biometric application.TOPIC: Real-time eye tracking for password authenticationAUTHORS: M. Mehrubeoglu and V. Nguyen PUBLICATION: IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2018, pp. 1-4, doi: 10.1109/ICCE.2018.8326302. Personal identification numbers are widely used for user authentication andsecurity.Password authentication using PINS requires users to physically input the PIN, which could be vulnerable to password cracking via shoulder surfing or thermal tracking.PIN authentication with hands-off gaze-based PIN entry techniques, on the other hand, leavesno physical footprints behind and therefore offer a more secure password entry option. • Gaze-based. authentication refers to finding the eye location across sequential image frames.and tracking eye center over time. Author presents a real- time application for gaze-based PIN entry, and eye detection andtracking for PIN identification using a smart camera.

CONCLUSION:

A camera based mostly eye-blinking system has been incorporated into a replacement application for palpebra blink-based PIN identification. The system has been with success tested with a nine-digit keyboard, and can be extended to character and digit combination secret entry. the steadiness of the user's physiological reaction can have an effect on the accuracy of the detected pins, and should be accounted. Currently, the PIN identification is

accomplished when period of time eye-blinks computations and recording are complete.

REFERENCES

Extensive study about the topic was performed and various methodologies used in this domain were found. Exploratory analysis visualizes events that have occurred in the past and provides meaningful insights that can be used for decision making.

[4] 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- jee/papers/Vol17-issue4/Version2/B017420915.pdf)

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

[6] M. Mehrubeoglu, E. Ortlieb, L.. McLauchlan, L. M.

[2] J. Weaver, K. Mock and B. Hoanca, "Gaze-Based Password Authentication through AutomaticClustering of Gaze Points," Proc. 2011 IEEE Conf. on Systems, Man and Cybernetics, Oct. 2011 (DOI: 10.1109/1CSMC.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.european- atm 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)

[7] 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".

[8] Smart Cameras for Embedded Machine Vision, (product information) National Instruments (Available: http://www.ni.com/pdf/products/us/cat ni 1742.pdf)