Available online @ https://jjem.jnnce.ac.in
https: www.doi.org/10.37314/JJEM.SP0247
Indexed in International Scientific Indiexing (ISI)
Impact factor: 1.395 for 2021-22
Published on: 08 December 2024

EYE PUPIL MOVEMMENT BASED PIN AUTHENTICATION SYSTEM

Karthik A S [1*], Manjunatha H T [2]

[1*]Student, Department of MCA, Jawaharlal Nehru New College of Engineering, Shivamogga, India.

[2]Assistant Professor, Department of MCA, Jawaharlal Nehru New College of Engineering, Shivamogga, India

karthikaskarthik4440@gmail.com, manjudeepa@jnnce.ac.in

Abstract

Nowadays critical data must be protected in the digital era with robust authentication methods, there are drawbacksand weaknesses to using conventional techniques like biometric authentication and alphanumeric password. The uniqueness and complexity of ocular behavior are leveraged in this paper. Revolutionary approach to password generation via eye pupil movement hence improving security. Technically the system collects data on pupil movementin real time by using an eye-tracking device to find distinctive patterns. In this data computer vision algorithms and machine learning methods are combined. The basic algorithm uses methods for feature extraction to convert the unprocessed eye movement data into a set of vectors and coordinates. They are then converted by a safe hash algorithm into a cryptographic key, guaranteeing that every password created is distinct and only repeatable by thatparticular user.

Keywords*: Face land mark detection, Haars cascade algorithm*

1. Introduction

Using the unique and involuntary patterns of a user's eye movements to confirm their identification the eye pupil movement-based pin authentication system is a creative and complex solution to biometric security ad vanced computer vision techniques especially face landmark identification and the haar cascade algorithm which combined allow exact tracking and analysis of eye movements are essential to this system. The initial step involves utilizing a camera to take a sequence of pictures or a live video feed of the users face then by scanning the image at various sizes and using a cascade of classifiers that effectively recognize the existence of a face the haar cascade technique is utilized to locate and isolate the face inside each frame the next critical step after detecting the face is detecting facial landmarks as reference points for isolating the eye regions this recognizing important face structures like themouth nose and eyes with great precision. Theselandmarks can be identified by con- temporary machine learning models like the ones included in the dlib toolkit the algorithm selects the eye- corresponding regions from the recognized landmarks and crops them out of the picture. Sothat it may be considered in more detail numerous pictures refining methods such thresholding though transformations or sophisticated depth in learning strategy are utilized by the system to identify and monitor the pupils within these isolated eye regions. The dependability of the authentication procedure depends on precise tracking of the movement of the detect- ed pupils.

2. Literature Survey

Panda, A et al [1] describes a system that utilizes a random forest classifier to authenticate users'

classification. The approach improves the accuracy of gaze tracking, which is crucial for reliable eye movement-based authentication systems. Wei Li, Lin Li, et al [7] develop a real-time eye pupil tracking system for biometric authentication. By using leading picture processing techniques, the system accurately detects and tracks pupil movements, demonstrating its potential for real-time security ap- plications. Introduce a gaze- based password authentication system that employs automatic clustering of eye movement aspect. Their method enhances security and usability by leveraging natural gaze behaviors, reducing the chance of forgery, and providing an intuitive method for user and authentication. Gives a prophetic ideal for eye movement biometrics in user authentication. Their research focuses on predicting and recognizing individual-specific eye movement patterns, which can be used for secure authentication. based on the eye movement pat- terns during PIN entry. The approach involves preprocessing eye movement data to extract features like fixation points and sac cades. By training the classifier on these features, the system distinguishes between legitimate users and imposters, enhancing security through biometric verification. Kumar, et al [2] proposed a secure PIN authentication system leveraging recurrent neural networks (RNNs) to model and analyze eye movement dynamics. The system preprocesses raw eye movement data to capture temporal dependencies and behavioral patterns. By training RNNs to recognize legitimate user patterns during PIN entry, the system aims to improve authentication accuracy and resist spoofing attacks. Lee, et al [3] represents a biometric authentication system tailored for smart devices, integrating eye movement analysis with traditional PIN verification. The system employs computer vision techniques for real- time pupil detection and tracking during PIN entry. By combining eye movement biometrics with PIN authentication, the system enhances security and usability on mobile and smart devices.X. Zhang, et al [4] propose an authentication system using a neural network ensemble to analyze eye movement data. The system pre-processes eye movement sequences and feeds them into multiple neural network models are gettrain to recognize unique user patterns. By integrating outputs from these models, the ensemble enhances authentication accuracy and robustness against variations in eye movement patterns'. Smith, et al [5] explore methods to strengthen traditional PIN-based authentication by incorporating eye movement biometrics. The system preprocesses eye movement data to extract features such as fixation durations and scan paths. numerical analysis techniques are occupied to authenticate users based on these biometric characteristics during PIN entry, improving security while maintaining user- friendly authentication processes. Sanghyun Park, et al [6] discusses an eye gaze tracking method that combines feature extractionwith Support Vector Machine (SVM).

3. Methodology

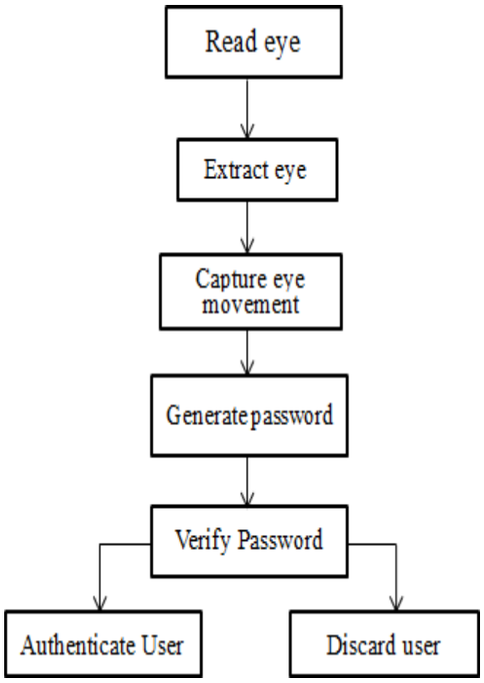

Figure 1: Blcok Diagram

3.1.1 Read Eye: Use high-resolution camera to record a sequence of eye pictures or video frames.

3.1.2 Extract Eye: The system processes the captured image to isolate the eye region.

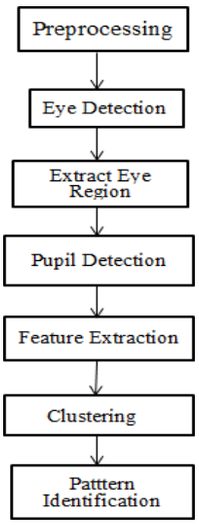

Figure 2: Work Flow Diagram

3.2.1 Preprocessing: The photos are first transformed to grayscale, which removes color information and concentrates only on intensity values, hence reducing the computing load. Noise reduction is then applied to minimize the random variations in pixel in- tensity and to smooth's the image using gussian blur.

3.2.2 Eye Detection: Haar cascade classifiers are employed in the eye detection stage to find the eye region in the image. Haar cascades swiftly search the image for pat- terns that correspond to previously taught eye models.

3.2.3 Extract Eye Region: After the eye region has been identified it is isolated by cropping the image to solely focus on the relevant area. This is an important stage since it finds the exact location of the eye, which is needed for feature extraction and accurate pupil identification.

3.2.4 Pupil Detection: Determining the radius and center of the pupil inside the cropped eye region. In order to make it easier to determine the shape of the pupil, edge detection techniques such as the canny edge detector are used to emphasize the pupil's boundaries. After identifying circular structures inside the edge-detected image and the pupil precise location and size are determined.

3.2.5Feature Extraction: Getting comprehensive data on the properties of the eye is the main goal of feature extraction. Important parameters including the radius, gaze direction, and center coordinates of the pupil are computed. In order to assess the size and form of the eye, ocular contours are identified. Blink patterns are then tracked by tracking variations in these contours over time.

3.2.6 Clustering: Clustering algorithms, such as k-means and DBSCAN, are applied to the collected features to group similar movement patterns. These algorithm helps in recognizing consistent patterns in eye movements, which are unique to each user. Clustering enables the system to differentiate be- tween different types of movements.

3.2.7 Pattern Identification: Entails comparing stored patterns with the eye movement patterns that are detected in order to verify the user's identity. The pre-stored patterns and the real-time detected patterns are compared using similarity metrics such Euclidean distance and Dynamic Time Warping.

3.1.3 Capture Eye Movement: The user eye Blinks are capture and recorded by system to make sure the user is engaging with authentication.

3.1.4 Generate PIN: The system creates adistinct pin based on identified ocular characteristics and blink patterns.

3.1.5 Verify PIN: The generated PIN is either asked to be entered by the user or it is com- pared to a stored value by the system.

3.1.6 Authenticate User: The user is given access and is verified if the PIN is entered correctly.

3.1.7 Discard user: The user is refused and access is forbidden in the event that the pin verification is unsuccessful.

4. Experimental Result

The experiment consists an eye efficient dataset to design and to assess a password authentication mechanism based on extensive image collection which documents number of movement pattern and forms of eye movement. The training and testing there were used 150 eye images. Such images include various eye movements that facilitate to generate password based on particular eye movement in various direction this offer more appropriate solution for password generation.

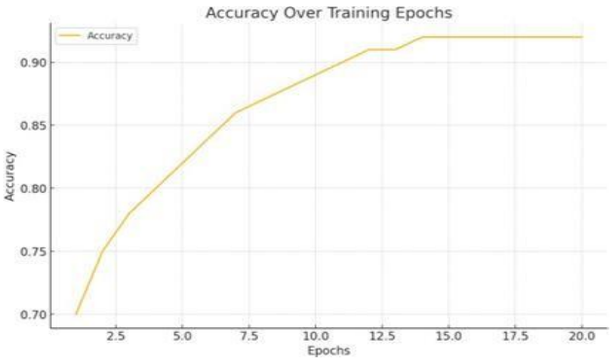

Figure 3: Accuracy Over Training Process

The fig 4.1 describes that the Model's accuracy was gain throughout the training process are displayed in the graph.

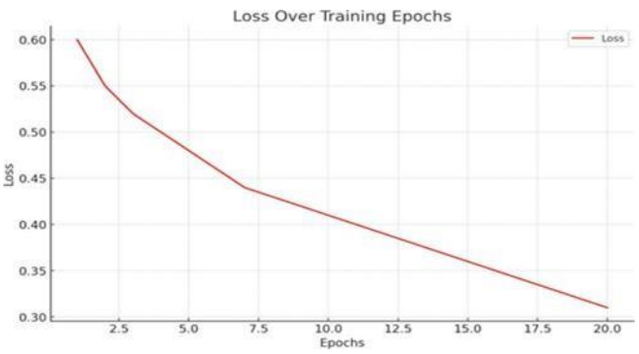

Figure 4: Loss Over Training Process

The fig 4 shows that the graph depicts the decrease in loss over the training Process, indicating the model's learning progress.

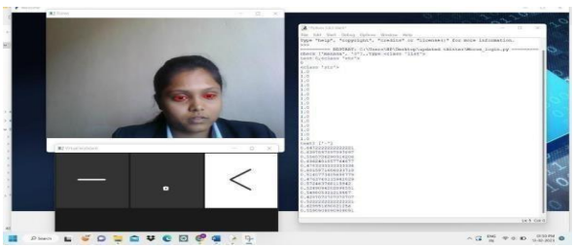

Figure 5: Password Entry by eye movement

The fig 5 shows that selecting of password through series of different morse code of each character and converts code to each character in password. Morse code is selected by eye movement done by the user.

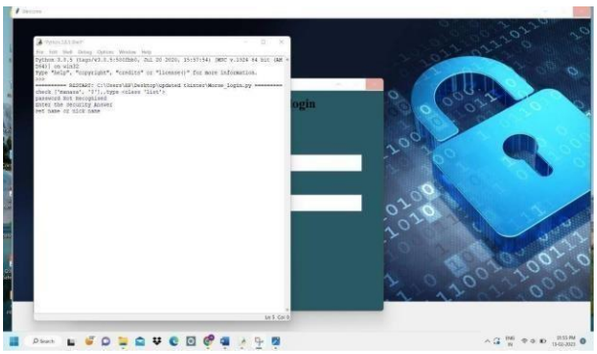

Figure 6: Movement Towards Password Generate

The fig 6 Shows that pin generated through morse code of each character in pass- word. The user can access file after entered password is correct. The Performance analysis with respect to Confusion matrix for the above methodology is shown in below Table 1.

Model	No. of images	TP	FP	TN	FN	Accuracy	F1 score
Eye images	150	80	10	50	10	0.91	0.92

Table 1: Performance Analysis

These results indicate that the system is highly effective at recognizing correct eye pupil movements for password generation, with minimal false detection. The low number of false positives and false negatives further support the reliability of this biometric authentication method.

Sl. No	Authors	Algorithm /Technology	Accuracy
1	Liu and Chang	Saccaic movement analysis	85%
2	Brown et al.	Eye blink pat- tern recognition	89%
3	Kim and lee	Convolution Neural network	90%
4	Our Method	Face landmark detection/haars cascade	93%

Table 2: Comparative Analysis

Table 2 gives the comparative analysis which contain different authors with different algorithms and technique used. On com- paring accuracy of others our work has gained more accuracy.

5. Conclusion

This work explores the novel use of face landmark detection techniques along with deeplearning and advanced image processing algorithms like Haar Cascade to generate passwords based on eye pupil movement. The research has developed a strong system for safe user authentication using distinctive eye movement patterns by employing a diverse dataset. The proposed method has demonstrated an impressive ac- curacy rate of approximately 92% in detecting and interpreting eye pupil movements under a variety of situations. The confusion matrix was one of the common evaluation measures used toconfirm the system's functionality. All in all, this research presents a novel and safe password.

generation mechanism that significantly advances biometric authentication. Thetechnique is expected to improve security protocols in high-security applications including financial transactions and personaldata security.

References

1. A. Panda,et.al.,“Advanced Safe PIN-Entry Against Human Shoulder Surfing,” IOSR Journal of ComputerEngineering.

2. B kumar,et.al.,“Gaze–Touch pass Scheme “,March 2016.

3. C. Lee, et al. “Real time Eye Gaze Direction Classification Using Convo- lutional Neural Network”, June2016.

4. X.Zhang,et.al.,“pin Type Using Eye Gaze to Enhance Typing Privacy”,May 2017.

5. J.Smith, et. al. “Survey Paper on Eye Gaze Tracking Methods and Techniques”.

6. Sanghy et.al.,"EyePupil Based PIN Authentication System Using Image Processing Techniques," 2018 In- ternational Conference on Computer, Communication, and Signal Processing (ICCCSP), pp. 1-5, 2018.

7. Qiong Zhang,et al.,"Pupil Detection Based on Gradient and Region Seg- mentation,"2012.