EOG-based Blink Authentication

Kaushik B[1], Vinay Kumar M[2], Ashish Vats[3], Sirisha Tadepalli[4]
Department of Electronics and Communication Engineering
Amrita School of Engineering, Bengaluru,
Amrita Vishwa Vidyapeetham, India
bl.en.u4ece19015@bl.students.amrita.edu[1], bl.en.u4ece19174@bl.students.amrita.edu[2],
bl.en.u4ece19013@bl.students.amrita.edu [3], t_sirisha@blr.amrita.edu[4]

***Abstract*— Advanced identity authentication methods that offer ease and security have been created as a result of the internet's widespread use and rising popularity of electronic gadgets. We are becoming more and more dependent on these devices, though, which increases the potential for spoofing and privacy violations. The static photographs of faces or fingerprints used in many current authentication systems make them susceptible to attacks utilizing fabricated data. To solve this problem, we offer a unique Dynamic Biometric Authentication System (DBAS) that integrates individual eye blink patterns with face authentication to increase system redundancy and security. The suggested system identifies the user using a variety of facial recognition techniques and then uses a unique blink pattern to confirm the user's identification. In this study, we offer an authentication system using eye-blinking Electro Oculo-gram (EOG) signals for safe person identification in response to the flaws in current authentication techniques. This system records blink signals using an Arduino-based EOG detection device and then extracts pertinent information from the data. In order to authenticate the participants, these traits are combined with a linear discriminant analysis (LDA) classifier.**

Keywords— Authentication, EOG, VOG, LDA

I. INTRODUCTION

Systems for secure and convenient identification and verification based on a person's physiological or behavioral features are now called biometric authentication systems (BAS) [1]. The security of these systems is jeopardized by the fact that traditional biometric features like fingerprints and facial features are susceptible to hacking and spoofing techniques [2]. To combat this problem, several anti-spoofing approaches have been developed, such as user interaction, contextual data methods, facial aliveness identification, texture evaluation, and face blinking [3]. Some of these methods, though, call for pricey detectors or outside sensors, which raises system costs and decreases system effectiveness.

Recently, eye-blinking has emerged as a promising biometric trait, particularly in applications like driver drowsiness detection, and it is an artifact in particular objective eye diagnosing devices [18]. Eye-blinking is advantageous because it is difficult to forge or capture at a distance, unlike fingerprints or faces [4]. Electrooculogram (EOG) signals have gained attention as they provide electrical recordings of eyeball and eyelid movements using electrodes around the eyes. EOG signals offer several advantages over traditional biometric traits, including resistance to forgery, ease of collection, and one-dimensional, low-frequency characteristics that facilitate efficient processing [4,17]. Expert neurologist Jesper Ronge has confirmed that eye blinking patterns are unique and can be readily collected using electrodes near the eyes.

This paper proposes a novel approach that integrates an eye-blinking system with an existing biometric face authentication and verification system to enhance biometric authentication and verification. This integrated approach, the dynamic biometric authentication system (DBAS), involves the analysis of eye-blinking movements using EOG signals [5]. By leveraging the unique characteristics of EOG signals and their correlation with individual eye-blink patterns, the proposed system aims to enhance the security and reliability of biometric authentication.

II. RELATED WORK

By adopting EOG (Electrooculography) and VOG (Videoculogram) techniques to record and transmit information on ocular rotation, biometric traits can be inferred. Many criteria and methods are utilized for identification, verification, and authentication to distinguish between EOG and VOG procedures [6]. A research study claims that choosing one validation method over the other provides greater security and user ease [7] even though a specific validation method isn't mentioned.

Utilizing methods like Haar-like characteristics, which categorize facial features including the eyes, nose, and mouth, facial-based authentication systems such as VOG or facial-based authentication systems begin by identifying faces in photos or videos. Calculations of the correlation coefficient and eye region extraction, and template matching are used. The combination of these approaches has demonstrated great face detection accuracy for applications involving human-machine communication, exceeding 99% [8].

Algorithms for facial recognition are integrated with dynamic features to improve security. Consequently, the suggested solution, DBAS, is divided into two independent phases [5]. In the first stage, the user's face is recognized and verified using the OpenCV and D-lib libraries. The technology emphasizes eye detection and eye blink authentication much more in the second stage of user authentication [5].

In EOG-based techniques, specialized electrode-equipped devices record the potential produced by eye or eyelid movements. Electrodes are positioned surrounding the eye to record EOG signals and track changes in the electric potential field brought on by eye movement [9].

The pre-processing module sets up the acquired data for analysis and feature extraction after the data acquisition device acts as the sensor for gathering biometric data. The feature extraction module focuses on extracting particular properties that successfully distinguish people from one another. In the identification setting, the system may determine the individual's identity based on these traits, and it can also either approve or decline the stated identity, enabling user authentication. [10].

This study conducted authentication in two layers: video image authentication and EOG authentication. For the former, various characteristics of the blink are extracted, and their correlation with other characteristics is studied to choose authentication features.

II. Methods and Results

A. *Dynamic biometric authentication system using the image and EOG eye blink detection systems:*

1) Face recognition

The proposed dynamic authentication system integrates face recognition and blink pattern detection. OpenCV and D-lib libraries are installed to implement the system, and the Haar cascade algorithm is utilized for object detection in images. The Haar cascade algorithm is a real-time feature-based object detection technique that does not require extensive computational resources. It utilizes the cascade function and cascading window to calculate features for each window, classifying them as positive or negative. However, it should be noted that the Haar cascade is limited to shape and size matching and cannot be used for face recognition.
Pre-trained Haar cascade files designed for human face detection are employed to overcome false positives. Additionally, the system incorporates the Linear Binary Pattern Histogram (LBPH), a well-established facial recognition algorithm capable of recognizing individuals from frontal and profile views.

The LBPH algorithm operates by examining a matrix representing a portion of an image. It partitions the image into squares and assigns different values to each square based on lighting conditions and RGB values. The algorithm starts processing from the top-left corner element, moving circularly as if creating a circle, including the first element of the second row, and so forth. This circular pattern enables the extraction of local texture information from the matrix representation of the image.

2) Video-based eye blink detection:

Using facial landmarks, OpenCV, and D-lib libraries, the eye blink pattern is discovered following face recognition [11,19,20]. The D-lib library is used to calculate the positions of 68 (x, y)-coordinates on the face that corresponds to different facial structures (Fig. 1). These coordinates are then used to localize and name particular facial features, including the lips, right and left eyebrows, the right and left eyes, the nose, and the jaw. When detecting eye blinks, each eye is represented by six (x, y)-coordinates arranged clockwise around the ocular region, starting at the left corner of the eye. It's essential to remember that these coordinates show a particular correlation between width and height.

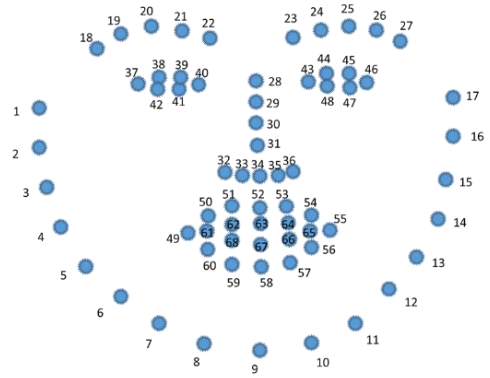

Fig. 1 Localization of facial points using D-lib library

The relationship between the six coordinates of the eye is captured by an equation known as the eye aspect ratio (EAR), which was developed based on the study done by Soukupová and Ech et al. [11]. The following is the EAR equation:

$$EAR = ||p2 - p6|| + ||p3 - p5|| / 2 * ||p1 - p4|| \quad (1)$$

The 2D face marker locations are represented by p1, p2, p3, p4, p5, and p6 in this case. The distance between the horizontal eye landmarks is calculated in the denominator of the equation, whereas the distance between the vertical eye landmarks is calculated in the numerator. The denominator is suitably weighted since there is only one set of horizontal points but two sets of vertical points.

The EAR fluctuates little when the eye is open but rapidly decreases to zero when the eye blinks. The EAR formula calculates the indices of both eyes and their EAR ratios individually. The needed blink pattern is then checked against the identified eyeblink patterns before being placed in an array and approved. The facial recognition and eye blink sequence detection criteria must both be met for authentication to be given.

B. *EOG-based eye blink authentication*

The eye blink data of different subjects are recorded by interfacing the Bio Amp-EXG-Pill amplifier (i.e., instrumentation amplifier, upside-down labs) with the Arduino. While blinking, the orbicular oculi muscles contracts and generates biopotentials. These biopotentials are detected by placing the electrodes at specific locations on top and down the eye and behind the ear as a reference or ground electrode, as shown in Fig. 4.

An EOG signal can be seen as the corneo-retinal potential (CRP). The detection of eye movements is possible using these EOG signals. When the eye moves from the center position toward one of the two electrodes, it experiences the retina's positive side; meanwhile, the opposite electrode experiences the retina's negative side. There is, thus, a potential difference between the electrodes. In the event that the resting potential is

consistent, the recorded potential serves as a marker for the eye's position.

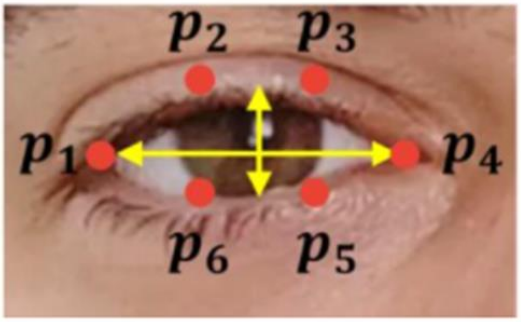

Fig. 2 Land points for evaluation of EAR ratio

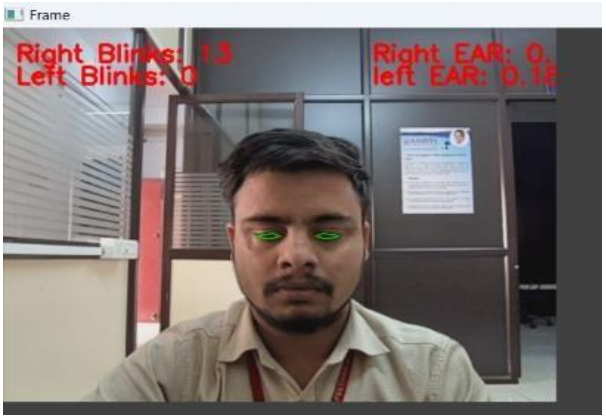

Fig. 3 Real-time video eye blink detection system by evaluating the EAR ratio

To record clean EOG signals, we need an analog serial out Arduino port with a fixed sampling rate of 75Hz. While recording the eye blinks, the noise in the signal is rectified by applying a fourth-order Butterworth IIR digital band-pass filter at a frequency range of 0.5 - 19.5 Hz.

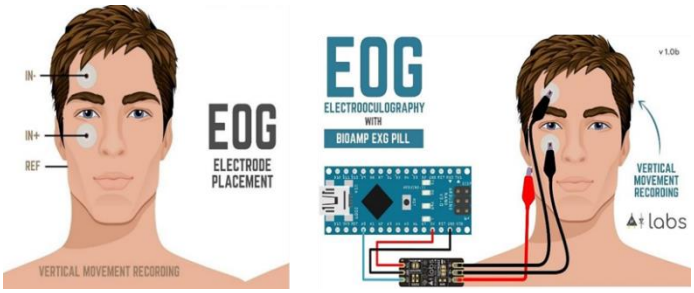

Figure. 4 Placement of electrodes for EOG recording [11

The study recorded the eye blink on 60 normal subjects (male = 51, average age = 21; female = 4, average age= 43). Fig. 6 shows the sample EOG blink signal of a normal subject that was recorded with a predefined interval and at a random interval for 30 seconds. After recording the data, the following steps are involved for the signal processing and feature extraction from the data.

1) Pre-processing of signal:

The first 250 and last 250 samples of data are deleted to remove redundant data. Then, 5% of the maximum and minimum are recorded. Based on these values, values less than 5% maximum and more than 5% of the minimum are deleted [12].

Fig. 5 Photograph of recording EOG blink signal on normal subjects

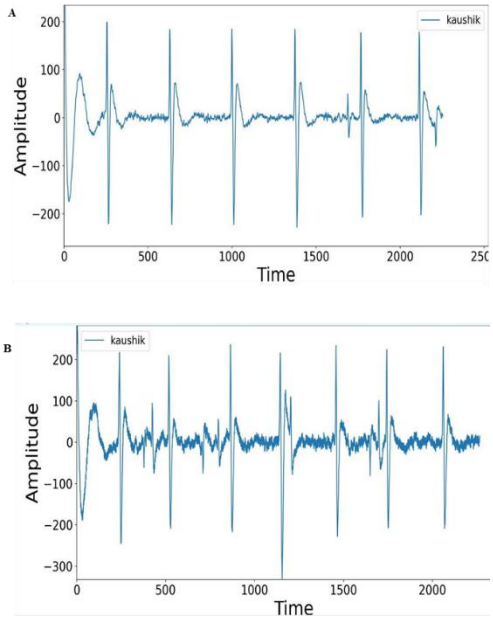

Fig. 6 A. Sample of EOG periodic blink signal of a normal subject for a duration of 30 seconds, B. Random blinks for a duration of 30 secs

2) Feature extraction:

Excel macros were developed to automate feature extraction. Positive and negative values greater than 90% of the maximum and less than 90% of the minimum are selected as the amplitude of positive and negative signals. Positions of positive and negative peaks are identified using the match function, duration of positive and negative is found using the subtotal function, energy of the signal is found by calculated parameters, and slope (tan) of onset and offset of both positive and negative is found. The extracted features are run through a feature importance

technique to extract the required features for more efficient and accurate authentication.

The average values of the seven features extracted are listed in the table below, respectively:

TABLE 1 Average values of all the extracted features

Name of the feature	Average value (n = 55)
Positive peak amplitude	260.78
Negative peak amplitude	-298.54
Area of the positive peak	1609.22
Area of the negative peak	1957.79
Energy of positive peak	9482.35
Energy of negative peak	9019.15
Slope of onset (Tan(θop))	38.90
Slope of offset (Tan(θ_{fo}))	41.53

However, all the features cannot be applied to the authentication. Therefore, the appropriate features are selected by evaluating their importance.

3) Feature selection:

In order to create the feature extraction CSV file, which is needed to train the classifier, the extracted features outlined above are concatenated for all the acquired test subjects. Some of these features could harm the performance of the classifier because they could not be exclusive to each subject. The addition of a feature selection strategy allows for the selection of a subset of the available features in order to reduce classifier error or increase classifier accuracy. To find the best level of accuracy for the smallest subset of features, a number of feature selection strategies were tested. The Differential Evolution (DE) method was determined to have the most properties that were appropriate for our suggested system. An algorithm for evolutionary optimization called DE is utilized to address optimization issues.

Accuracy and the search strategy are the two most crucial aspects that should be taken into account for a feature selection technique [10]. Seven sets of the properties from Table 1 were ultimately chosen as potential applications for blink authentication. On the contrary, all 14 features were taken into account to ensure that the suggested authentication solution was as accurate and reliable as possible.

4) Classifier

Linear Discriminant Analysis (LDA) was chosen for classification due to its popularity in machine learning and pattern recognition. It is a supervised learning algorithm that aims to find a linear combination of features that maximizes the separation between different classes while minimizing the within-class scatter. Using LDA, the accuracy for face recognition, document classification, and anomaly detection was about 80%, the highest among other classifiers.

The Heat map (see Fig. 7) shows the correlation among all the 14 features evaluated from the recorded blink signals. It is observed that four features of a correlation factor above 0.75 can be considered for feature selection. However, it is later revealed that the selected features do not provide the desired accuracy, which persuades us to consider all 14 features for higher accuracy. From Fig. 8, it is evident that variation in accuracy with respect to the number of features is higher with an increase in the number of features. Therefore, for better accuracy, we have considered all 14 features for authentication. Also, as the number of subjects is increasing, the authentication accuracy was moderate to lower.

III. DISCUSSION

Blink authentication has greater biological significance and personal encryption than other explicit biometrics. Biological currents cause the unconscious movement of blinking [13]. Simple eye movements have been found in studies to improve information extraction. Additionally, users are often at ease keeping a steady face, given how facial recognition systems are being developed.

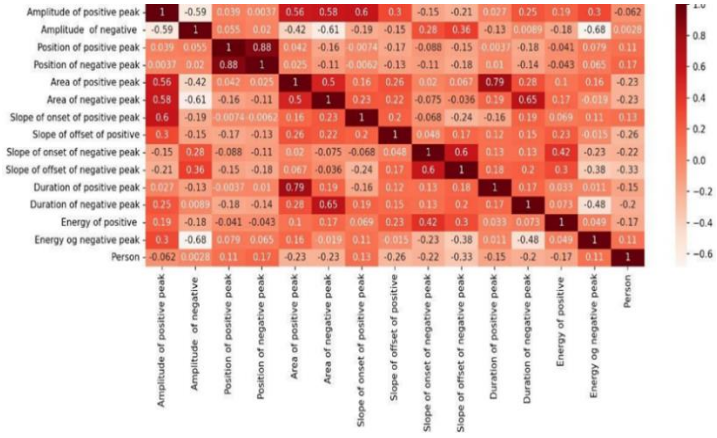

Fig. 7 Heat map for feature selection

It has been proposed that by utilizing motion compensation or prior information, ocular movements can be separated from synthetic movements that coincide with facial and eye motions [13]. Depending on the needs of various users or application scenarios, the system usability and security level can be traded off.

Our suggested authentication technique is straightforward and inexpensive, as just one bio-amplifier sensor is required to record a subject's natural eye blinks. The recommended method successfully recognizes users for a population of more than 60

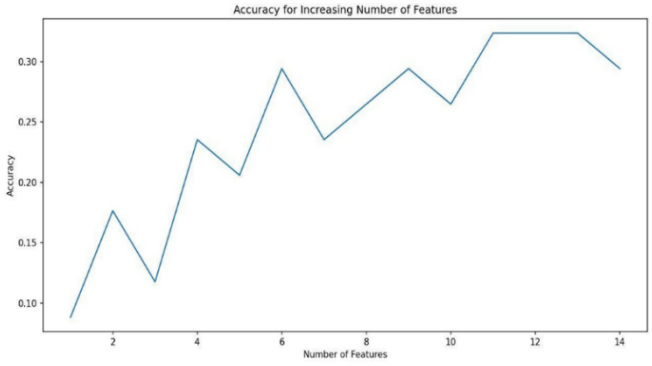

Fig. 8 Variation of accuracy by increasing the number of features

participants with an accuracy of up to 80% using filtered EOG signals to extract essential elements from the eye-blinking

waveform. Despite the optimistic results, there are exceptions and cautions according to thorough research on the suggested approach.

The trials suggest that this proposed biometric method is not as well-suited as previously believed for identifying a variety of participants' eye blinking patterns. It is also noteworthy that even when taking into account many basic classifiers, the system's performance noticeably decreases to as low as 30% when dealing with the eye blinking of more than 20 participants. It was found that LDA had the highest accuracy of the many classifiers examined, including SVM, KNN, and others.

There are likewise few changes when the number of attributes examined across several people is taken into account. This is most likely because there is little to no difference in the number of features with a high subject count, suggesting that the properties of blinks are constant among subjects with more than 30. The methods used in this study may not perfectly abstract the methods used in other related research papers or the methods used for various signal extraction techniques like EEG and ECG waveforms, which are more sophisticated and clearly defined as biometric signals. This highlights the need for better methods for extracting and gathering EOG eye-blinking waveforms.

In order to evaluate the eye-blinking waveform's ability to distinguish between users, it is imperative to comprehend the diversity in the properties of EOG blink waveforms across a larger population, including thousands of users. The performance of the system may also be improved by gathering training samples for the same user utilizing a more reliable approach for data collection of EOG eye blinking waveforms.

The intensity of the eye-blinking waveform may be influenced by various factors, such as attentiveness or exhaustion, which may impact authentication. Future research must take these concerns into account.

IV. Conclusion

Numerous feature extraction procedures might be assessed and contrasted with those suggested because no system is fault-proof. The suggested biometric authentication system can be made more effective and secure by taking into account how eye-blinking EOG signals can be combined with additional features like EEG signals to create a multimodal system. Despite the promising results from the simulations, eye-blinking EOG signals still need more study to overcome the aforementioned issues. These signals may only be regarded as trustworthy biometric traits for verifying human identity.

Future exploration can involve the development of new measurement devices, such as designing glasses with embedded sensors or utilizing different sensor technologies to measure blinking. These advancements may contribute to improving the accuracy and reliability of eye-blink authentication systems.

V. Acknowledgement

The Visvesvaraya Graduate Scheme for Technology (VGST), Karnataka state, India, provided financial support under Award No. VGST/K-FIST (L1) (2020-21)/2021-22/879.

References

[1] Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security, 1(2), 125–143.

[2] Singh, S., & Prasad, S. V. A. V. (2018). Techniques and challenges of face recognition: A Critical Review. Procedia Computer Science, 143, 536–543.

[3] Komulainen, Jukka, Abdenour Hadid, and Matti Pietikäinen. "Context-based face anti-spoofing." 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE, 2013.

[4] Abo-Zahhad, Mohammed, Sabah Mohammed Ahmed, and Sherif Nagib Abbas. "State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals. IET Biometrics 4 (3), 179–190 (2015)." (2014).

[5] Saied, Marwa, Ayman Elshenawy, and Mohamed M. Ezz. "A Novel Approach for Improving Dynamic Biometric Authentication and Verification of Human Using Eye Blinking Movement." Wireless Personal Communications 115 (2020): 859-876.

[6] King, D. E. (2009). Dlib-ml: A machine learning toolkit. Journal of Machine Learning Research, 10, 1755–1758.

[7] Chen, Guang, et al. "NeuroBiometric: an eye blink based biometric authentication system using an event-based neuromorphic vision sensor." IEEE/CAA Journal of Automatica Sinica

[8] Królak, Aleksandra, and Paweł Strumiłło. "Eye-blink detection system for human-computer interaction." Universal Access in the Information Society 11 (2012): 409-419.

[9] Merino, Manuel, et al. "A method of EOG signal processing to detect the direction of eye movements." 2010 First International Conference on Sensor Device Technologies and Applications. IEEE, 2010.

[10] Kawasaki, Yohei, and Yuta Sugiura. "Personal Identification and Authentication Using Blink with Smart Glasses." 2022 61st Annual Conference of the Society of Instrument and Control Engineers (SICE). IEEE, 2022.

[11] Soukupova, Tereza, and Jan Cech. "Eye blink detection using facial landmarks." 21st computer vision winter workshop, Rimske Toplice, Slovenia. 2016.

[12] https://github.com/upsidedownlabs/BioAmp-EXG-Pill

[13] Abbas, Sharif N., and M. Abo-Zahhad. "Eye blinking EOG signals as biometrics." Biometric Security and Privacy: Opportunities & Challenges in The Big Data Era (2017): 121-140.

[14] Mahesh, T. R., et al. "Real-Time Eye Blinking for Password Authentication." International Conference on Intelligent Emerging Methods of Artificial Intelligence & Cloud Computing: Proceedings of IEMAICLOUD 2021. Cham: Springer International Publishing, 2022.s

[15] López, Alberto, et al. "Comparison of classification techniques for the control of EOG-based HCIs." Biomedical Signal Processing and Control 80 (2023): 104263.

[16] Jalilifard, Amir, et al. "Use of spontaneous blinking for application in human authentication." Engineering Science and Technology, an International Journal 23.4 (2020): 903-910.

[17] J. Amudha, S. Reddy, R., and Y. Reddy, S., "Blink Analysis using Eye gaze tracker", in Intelligent Systems Technologies and Applications 2016, J. Manuel Cor Rodriguez, Mitra, S., Thampi, S. M., and El-Alfy, E. - S., Eds. Cham: Springer International Publishing, 2016, pp. 237–244.

[18] Tadepalli, Sirisha, et al. "Reliability of aqueous flare measurements during uveitis by a spot fluorometer." Journal of ocular pharmacology and therapeutics 38.1 (2022): 66-73.

[19] Senthilkumar, T., and S. Veluchamy. "Performance Analysis of Hierarchical Face Recognition." The International Journal of Science and Technology 2.4 (2014): 299.

[20] Archana, M. C. P., C. K. Nitish, and Sandhya Harikumar. "Real-time face detection and optimal face mapping for online classes." Journal of Physics: Conference Series. Vol. 2161. No. 1. IOP Publishing, 2022.