

Electroencephalography biometric authentication using eye blink artifacts

Thamang Teddy Madile¹, Hlomani B. Hlomani², Irina Zlotnikova²

¹Letshego Botswana, Gaborone, Botswana

²Department of Computing and Informatics, School of Pure and Applied Sciences, Botswana International University of Science and Technology, Palapye, Botswana

Article Info

Article history:

Received Jun 5, 2024

Revised Jul 31, 2024

Accepted Aug 5, 2024

Keywords:

Biometric authentication

EEG

Eye blink artifacts

NeuroSky Mindwave Mobile

Pattern matching algorithm

ABSTRACT

This study presents a novel approach to electroencephalography (EEG) biometric authentication using eye blink artifacts. Unlike traditional methods that rely on imagination and mental tasks, which are susceptible to emotional and physical variations, this approach leverages the consistent effects of eye blinks on brainwaves for authentication. Brainwaves were recorded using the NeuroSky Mindwave Mobile 2 headset, and eye blinks were extracted via NeuroSky's blink detection algorithm. An authentication algorithm was developed based on blink strength, time, and frequency. The proposed method demonstrated high performance with an accuracy (ACC) of 97%, a false acceptance rate (FAR) of 5%, and a false rejection rate (FRR) of 1%. This study also explored the impact of emotions and physical exercise on the authentication process, confirming the method's robustness under varying conditions. These findings suggest that eye blink artifacts offer a reliable and practical biometric trait for EEG-based authentication systems, providing a secure alternative to traditional biometric methods. The substantial contribution of this research lies in demonstrating the superior stability and usability of eye blink-based EEG authentication under diverse conditions, compared to existing EEG authentication methods that often require mental tasks or multi-channel recordings.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Irina Zlotnikova

Department of Computing and Informatics, School of Pure and Applied Sciences

Botswana International University of Science and Technology

10071 Boseja, Palapye, Botswana

Email: zlotnikovai@biust.ac.bw

1. INTRODUCTION

This study presents a novel approach to electroencephalography (EEG) biometric authentication using eye blink artifacts. Unlike traditional methods that rely on imagination and mental tasks, which are susceptible to emotional and physical variations, this approach leverages the consistent effects of eye blinks on brainwaves for authentication.

Background to the study: biometrics refers to measurable physiological or behavioral traits for identity authentication [1]. EEG signals from brain activities offer unique, non-replicable biometric data despite being affected by emotional and environmental factors [2], [3]. Hidden biometric features, instead of visual structural features, allow for reliable identification while reducing the chances of forgery [4].

EEG is a dynamic, non-invasive, and relatively inexpensive technique used to monitor brain electrical activity in micro-voltages [5]. EEG signals are biopotentials formed from brain activities [6], [7]. Despite their complexity and susceptibility to noise from muscle movements and eye blinking, EEG signals

provide unique and non-replicable data, offering advantages over ordinary biometric data [2]. Biometric authentication using brainwaves differentiates clients from impostors based on distinctive EEG features [3], [8]. Electrical impulses from neurons are measured through electrodes attached to an individual's head [6], [9], and processed by a computer system.

One EEG biometric authentication method uses changes in brain signals due to eye blinks, typically occurring at a rate of 12-19 per minute. These can be monitored for abnormal patterns to detect unusual situations [10]. When an eye blink occurs, the eyeball rotates within its axis, creating a waveform that can be extracted from electrooculogram signals for identification tasks [11]. This rotation causes a large electric signal captured by electrodes, with eyelid closure leading to a positive deflection and opening to a negative deflection in the EEG waveform. Espinosa *et al.* [12] analyzed various physical magnitudes involved in eye blinking-position, speed, eyelid acceleration, power, work, and mechanical impulse. These features describe the physiological phenomenon of eye blinking and can be used for biometric authentication. The process typically includes an enrollment stage where an individual's EEG signal is recorded and stored. During authentication, the signal is recorded and matched using pattern-matching algorithms against the previously recorded signal [11], [13], [14].

An overview of the existing studies on EEG in biometric authentication: studies on the use of EEG in human biometric authentication can be categorized into two groups. The first group includes the methods of human biometric authentication that rely only on one EEG-related biometric trait (single-factor authentication). In contrast, in the second group, the methods employ several forms of biometric authentication including EEG (multi-factor authentication).

Single-factor authentication: in the first group, single-factor authentication, Chuang *et al.* [15] demonstrated that single-channel consumer-grade EEG sensors could achieve 99% authentication accuracy, comparable to multi-channel clinical-grade devices. The study highlighted improved usability and varied user preferences for different mental tasks but did not address scalability to larger, diverse populations or long-term usability.

Abo-Zahhad *et al.* [16] developed an EEG-based biometric identifier using eye-blinking waveforms, achieving high recognition rates with empirical mode decomposition and direct extraction methods from 25 subjects using NeuroSky Mindwave headsets. While demonstrating the feasibility of eye-blink signals for authentication, the study relied on small sample size, did not consider other EEG artifacts, and required frequent blinking, reducing practicality.

La Rocca *et al.* [7] achieved up to 100% recognition accuracy by fusing spectral coherence-based connectivity between brain regions as a biometric feature in eyes-closed (EC) and eyes-open (EO) conditions, outperforming power-spectrum measurements. Despite high accuracy, the study was limited by specific conditions (EC and EO) and a small dataset, with no discussion on generalizability to real-world scenarios.

Chen *et al.* [17] developed an EEG-based authentication system using the rapid serial visual presentation paradigm, achieving a 100% true acceptance rate for 29 subjects with average log-in times of 13.5 seconds for wet and 27 seconds for dry electrodes. However, the study did not extensively compare long-term performance or address stability and usability issues.

Liew *et al.* [18] proposed the incremental fuzzy-rough nearest neighbor (IncFRNN) technique for biometric authentication using visual evoked potentials, achieving superior performance to the incremental k-nearest neighbor (KNN) technique in accuracy, area under the receiver operating characteristic curve (AUC), and Cohen's kappa coefficient, with efficient model adaptation through incremental updates and minimal initial training data. The study showed the effectiveness of the IncFRNN technique but did not address performance in different environmental conditions or applicability to a diverse user base.

Gupta *et al.* [14] proposed an EEG authentication method based on eye blink impact, using a dataset from 20 subjects and employing multi-class classification with radial basis function support vector machine (RBF SVM) trained on features extracted via principal component analysis, including mean, variance, peak, duration, area, Fourier transform, and energy. While results showed that blink signals could accurately distinguish users, the dataset included only 20 subjects.

Jalilifard *et al.* [13] demonstrated that involuntary blinking signals could authenticate individuals with up to 98.7% accuracy using EEG data from 46 subjects, analyzed with statistical methods and the gated recurrent unit (GRU). This study was limited by its sample size, controlled conditions, lack of comparison with other methods, unexplored feature set impacts, unaddressed long-term stability, and potential EEG artifacts affecting authentication reliability.

Balci [19] proposed an EEG identification system involving signal reception, frequency decomposition, binary random forest feature selection, and classification with a hybrid multilayer perceptron-long short-term memory (LSTM-MLP) algorithm, suggesting its potential for closed systems with limited users. The study was limited by its applicability primarily to closed systems with a limited number of users.

Hernández-Álvarez *et al.* [20] designed an EEG-based authentication system using one-class and multi-class classifiers, specifically isolation forest and local outlier factor, and identified key EEG channels and brainwaves, comparing their contributions to traditional dimensionality reduction techniques like PCA and χ^2 tests. The study did not address the long-term stability and generalizability of the proposed EEG-based authentication system across diverse and larger populations.

Yap *et al.* [21] demonstrated that deep learning models, particularly through transfer learning, significantly improve EEG-based authentication performance over traditional methods like SVM and linear discriminant analysis (LDA) by effectively handling the non-linear and time-varying nature of EEG signals. However, the authors did not thoroughly investigate the real-time applicability, computational efficiency, or transferability of models across different EEG devices and configurations.

Multi-factor authentication: in the second group, multi-factor authentication, Abo-Zahhad *et al.* [22] proposed a multi-level EEG authentication technique combining eye-blinking brainwaves with those from visual stimulation and relaxation. This significantly improved recognition accuracy and error rates compared to using only eye-blink artifacts. However, the small sample size of 31 subjects limits its generalizability, and the technique needs validation across diverse tasks and larger populations.

Ruiz-Blondet *et al.* [23] developed the cognitive event-related biometric recognition (CEREBRE) protocol, using event-related potentials (ERPs) to elicit unique responses from various brain systems, achieving 100% identification accuracy for 50 users by controlling the cognitive state through a designed challenge protocol. Despite high accuracy, real-world performance and the impact of varying cognitive states and external distractions on authentication accuracy were not explored.

Wu *et al.* [24] combined EEG and eye-blinking signals in a multi-task authentication system, improving accuracy from 92.4% to 97.6% and demonstrating effective open-set authentication with a false rejection rate (FRR) of 3.90% and a false acceptance rate (FAR) of 3.87%. The system's complexity may impact usability and real-time performance, and validation on larger, more diverse populations is needed.

Zeng *et al.* [25] proposed an EEG-based identity authentication framework using face image-based rapid serial visual (RSV) presentation, achieving 94.26% accuracy within 6 seconds and 88.88% over 30 days by combining face and EEG traits with hierarchical discriminant component analysis and genetic algorithm optimization. The decrease in accuracy over time indicates potential issues with long-term stability, and more research is needed to optimize the number of EEG channels for practical use.

Wu *et al.* [26] proposed an EEG authentication framework using motor imagery, integrating signal preprocessing, channel selection, and deep learning classification to provide end-to-end authentication. This framework is typically used in motor imagery brain-computer interfaces for those with neuronal disorders. The study needs validation across a broader range of tasks and user demographics, and practical implementation and real-time performance were not detailed.

TajDini *et al.* [27] investigated user authentication using brainwaves influenced by blinking, attention, and emotion sequences, analyzing 40 features from ten electrode placements and employing SVM and AdaBoost to create a robust classifier. The study did not address the impact on user comfort and practical deployment, and further investigation is needed on the robustness of the extracted features across different environmental conditions and user states.

Beyrouthy *et al.* [28] leveraged 5G technology in multi-factor EEG-based authentication to enhance data transmission and processing, enabling real-time, remote authentication. However, potential security and privacy issues associated with real-time remote authentication and the impact of network latency on performance were not fully explored.

Krishnamoorthy and Raju [29] combined lip movement and electrocardiogram (ECG) data in a multimodal biometric authentication system, leveraging ECG's robustness against spoofing and fine-grained behavioral cues from lip movements. The research had limitations, including the focus on only two modalities, potential environmental noise impact on lip data, and a lack of extensive real-world testing. Additionally, computational complexity and practical challenges posed drawbacks for real-time application and widespread adoption.

Limitations of the existing studies: in addition to the gaps in specific existing methods, general observations indicate significant limitations. According to Alsumari *et al.* [30], most EEG-based recognition methods use signals from multiple channels or extended time frames, limiting their usability in real-life security systems. These methods often use hand-engineered techniques and do not generalize well to unknown data. Deep learning-based EEG recognition methods suffer from overfitting and require learning from small datasets [30]. Balcı [19] notes that the main reason EEG-based identification systems are not widespread is their unstable accuracy performance.

EEG-based authentication methods provide high security, permanence, and recognition accuracy but are usually tested in controlled lab environments. Al-Shargie *et al.* [31] showed that mental stress significantly impacts EEG. Studies [32]-[34] proved that emotions could destabilize brain responses, and

physical exercises also affect EEG authentication [35], [36]. However, eye blink artifacts in EEG waveforms remain consistent despite changes in cerebral activity [37]. Methods combining eye blink and EEG, such as those by Abo-Zahhad *et al.* [11] and Wu *et al.* [24], rely on cerebral activity, making them susceptible to physiological and psychological factors. Thus, eye blink-based authentication methods need further exploration for their practicality and usability, offering the same security advantages as EEG.

Study contribution: this study introduced a method using the effect of eye blinks on brainwaves for biometric authentication. Traditional EEG-based methods often rely on mental tasks or multi-channel recordings, making them susceptible to emotional and physical variations and less practical for real-life applications. In contrast, this method leverages the natural and consistent phenomenon of eye blinks, offering a more stable and user-friendly approach.

The main objective is to develop and validate a novel biometric authentication method using EEG signals influenced by eye blink artifacts. Specific objectives (SO) include:

- SO1: efficient and accurate capture of EEG signals and eye blink detection using the NeuroSky Mindwave Mobile 2 headset, ensuring a cost-effective and user-friendly setup.
- SO2: development of a robust authentication algorithm to identify individuals based on blink strength, time, and frequency features extracted from the EEG signals.
- SO3: ensuring high authentication accuracy and reliability, aiming for at least 97% accuracy, a false acceptance rate (FAR) of no more than 5%, and a false rejection rate (FRR) of no more than 1%.
- SO4: evaluating the impact of emotional states and physical exercise on authentication performance to ensure robustness under varying conditions.

Brainwaves were recorded using the NeuroSky Mindwave Mobile 2 headset, with the NeuroSky blink detection algorithm extracting eye blinks and their properties. Despite using a single-factor EEG-based authentication, the proposed algorithm's performance is comparable to other EEG-based algorithms. The paper includes an introduction outlining the problem, a method section detailing the experimental setup and algorithm development, a results and discussion section presenting the key findings, including the evaluation of the proposed algorithm performance, and a conclusion and recommendations section highlighting practical implications and future research directions.

2. METHOD

2.1. Experimental setup

The experimental setup used the NeuroSky Mindwave Mobile 2 headset to capture EEG signals, with the electrode positioned at Fp1 above the left eye. The forehead was prepped with an abrasive gel to minimize impedance. Signals were transmitted via Bluetooth to a computer with the ThinkGear connector tool. The raw EEG signals underwent pre-processing, including low-pass, high-pass, and notch filtering. Signals were classified into various brainwave forms, sampled at 512 Hz, and converted to 12-bit digital values. Features like blink time, strength, and number were extracted. During enrollment, features were stored in a MySQL database, and new data was compared using a pattern-matching algorithm.

2.2. The proposed method of EEG biometric authentication using eye blink artifacts

The EEG human biometric authentication method using eye blink artifacts proposed in this research consists of two phases—enrollment and authentication. The first three sub-phases in each phase are the same—signal capturing, signal pre-processing, and feature extraction. The last, fourth, sub-phase of the enrollment phase is user enrollment whereas in the authentication phase, it is user authentication.

2.2.1. EEG signal capturing

Capturing EEG signals in both enrollment and authentication phases involved three critical steps. First, electrode impedance was minimized by preparing the subject's forehead with abrasive gel to ensure a clean and stable connection. Second, the EEG signal was extracted using the NeuroSky Mindwave Mobile 2 device, positioned at the Fp1 location for optimal signal detection. Finally, the EEG data was recorded and transmitted via Bluetooth to a computer equipped with the ThinkGear connector tool for further processing and analysis.

2.2.2. EEG signal pre-processing

In both enrollment and authentication phases, captured raw EEG signals were forwarded for pre-processing to the ThinkGear AM (TGAM) module of the NeuroSky Mindwave Mobile 2 device. The TGAT chip embedded in the TGAM module was used to filter out the noise and separate EEG signals into different types of brainwaves. The signals were further classified by other built-in filters according to the brainwave frequency as delta (0.5 to 4 Hz), theta (4 to 7 Hz), alpha (8 to 12 Hz), sigma (12 to 16 Hz), beta

(13 to 30 Hz), and gamma (above 30 Hz) brainwave forms. Sampling was performed at 512 Hz; after that, the 12-bit resolution data was sent to the analog-to-digital converter (ADC). This process produced digital values for each type of brainwave.

2.2.3. Feature extraction

The proposed authentication algorithm focused on extracting eye blink features from pre-processed EEG data. The selected features were blink time, blink strength, and the number of blinks. Blink time (in milliseconds) indicates the timestamp of received packets. Blink strength, ranging from 1 (weakest) to 255 (strongest), measured blink intensity. Three sub-features-soft-blink, normal-blink, and hard-blink-were derived using the NeuroSky API. Since an average person blinks 15-20 times per minute, the number of blinks per second is approximately 0.25-0.33. This translates to two to four eye blinks in the 10-second timeframe used for capturing enrollment and authentication data.

2.2.4. User enrollment and authentication

In the enrollment phase, the data was recorded from a user in a 10-second timeframe, processed, and stored in the MySQL database as shown in subsections 2.2.1-2.2.3. Blink features blink time, blink strength, and the number of blinks that were continuously saved in memory. At the end of the 10 seconds, the data (blink time, blink strength, and the total number of blinks) was stored in a MySQL database. In the authentication phase, the same data was recorded from a user within the same timeframe of 10 seconds, and the blink features were extracted. After that, the authentication data was compared with the data stored in the database using the pattern-matching algorithm. The pattern-matching algorithm calculated the difference and gave scores/results on a scale of 0 to 100, where 0 indicated no match and 100 indicated a full match. The user was either authenticated or rejected based on a defined threshold value of 70.

2.3. Pattern matching algorithm

The pattern-matching algorithm compared blink time, blink strength, and the number of blinks between the authentication phase data and the stored database records. Blink time contributed 60% to the overall score, blink strength 30%, and the number of blinks 10%. At the start of the authentication phase, a timestamp was captured, and subsequent blink occurrences were recorded in milliseconds. The algorithm queried the database for stored blink times and matched them within ± 800 milliseconds, awarding a score for each successful match. The total score was based on the number of blinks captured during enrollment and authentication (two to four blinks in a 10-second timeframe). For each detected blink, blink strength values were recorded and compared to stored data within a range of ± 15 milliseconds. Successful matches contributed to 30% of the overall score, evenly divided across the total blinks. The number of blinks was calculated similarly and used to estimate scores for blink time and strength. The authentication phase blink count was compared with the enrollment phase data, awarding 10% if they matched. If not, the algorithm continued with other features, ensuring comprehensive verification.

2.4. Data quality assurance

All captured EEG signals underwent preprocessing to filter out noise and artifacts, including the application of low-pass, high-pass, and notch filters. Data points that exhibited excessive noise, interference, or incomplete signal capture were excluded from the analysis to maintain the integrity of the dataset. Only high-quality data, characterized by clear and consistent eye blink artifacts, were included in the final analysis, ensuring that our findings are both robust and replicable.

3. RESULTS AND DISCUSSION

3.1. Results and discussion of the application of the proposed authentication algorithm

For the proposed authentication algorithm, 10 subjects were recruited. Five were adult females aged 20–35 years, and the other five were adult males in the same age range. The authentication algorithm results for 10 subjects and 10 impostors with 10 trials are shown in Table 1. The two categories of participants are denoted as “sub” and “imp” for subjects and impostors, respectively.

The highest average score for an impostor was 61.2, below the acceptance threshold of 70. The score correlated with the complexity of the authentication pattern, defined by the number of blinks. Fewer blinks indicated a less complex pattern. Impostor 1, mimicking subject 1 with the lowest number of blinks (four), scored 61.2. Similarly, Impostor 10, mimicking subject 10 with five blinks, scored 49.2. This shows that pattern complexity affects algorithm performance. In the last two trials, subjects outperformed impostors. Subjects 4, 5, 7, and 9 achieved perfect scores of 100 in trial 9, while subjects 4, 7, and 10 did so in trial 10, likely due to their experience from previous trials.

Table 1. The authentication algorithm results

| Subject ID | No. of blinks | Trial 1 | Trial 2 | Trial 3 | Trial 4 | Trial 5 | Trial 6 | Trial 7 | Trial 8 | Trial 9 | Trial 10 | Average Score |
|------------|---------------|---------|---------|---------|---------|---------|---------|---------|---------|---------|----------|---------------|
| sub1 | 4 | 77 | 77 | 91 | 77 | 70 | 70 | 77 | 77 | 84 | 25 | 72.5 |
| imp1 | - | 61 | 46 | 68 | 61 | 76 | 61 | 62 | 69 | 54 | 54 | 61.2 |
| sub2 | 11 | 94 | 97 | 94 | 97 | 94 | 85 | 94 | 97 | 97 | 88 | 93.7 |
| imp2 | - | 0 | 0 | 0 | 82 | 0 | 0 | 63 | 0 | 0 | 63 | 20.8 |
| sub3 | 8 | 84 | 87 | 84 | 81 | 84 | 90 | 87 | 87 | 78 | 84 | 84.6 |
| imp3 | - | 33 | 0 | 0 | 33 | 26 | 0 | 57 | 29 | 32 | 32 | 24.2 |
| sub4 | 6 | 85 | 85 | 90 | 95 | 90 | 90 | 95 | 95 | 100 | 100 | 92.5 |
| imp4 | - | 60 | 55 | 60 | 55 | 0 | 60 | 45 | 40 | 50 | 30 | 45.5 |
| sub5 | 8 | 92.5 | 92.5 | 96.25 | 88.75 | 92.5 | 92.5 | 92.5 | 92.5 | 100 | 96.25 | 93.6 |
| imp5 | - | 47.5 | 25 | 62.5 | 58.75 | 28.75 | 25 | 58.75 | 25 | 73.5 | 62.5 | 46.7 |
| sub6 | 8 | 92.5 | 92.5 | 88.75 | 88.75 | 88.75 | 92.5 | 96.25 | 96.25 | 92.5 | 96.25 | 92.5 |
| imp6 | - | 58.75 | 58.75 | 40 | 32.5 | 47.5 | 28.75 | 32.5 | 32.5 | 40 | 17.5 | 38.7 |
| sub7 | 6 | 85 | 100 | 90 | 95 | 90 | 90 | 90 | 100 | 100 | 100 | 94.0 |
| imp7 | - | 30 | 90 | 30 | 55 | 40 | 35 | 40 | 35 | 50 | 40 | 45.5 |
| sub8 | 9 | 88.75 | 85 | 88.75 | 88.75 | 85 | 92.5 | 88.75 | 88.75 | 92.5 | 92.5 | 89.1 |
| imp8 | - | 0 | 55 | 66.5 | 58.75 | 62.6 | 47.5 | 0 | 62.5 | 47.5 | 51.25 | 45.1 |
| sub9 | 8 | 85 | 92.5 | 92.5 | 92.5 | 85 | 81.25 | 96.25 | 96.25 | 100 | 96.25 | 91.7 |
| imp9 | - | 0 | 0 | 58.75 | 0 | 0 | 0 | 58.75 | 66.25 | 58.75 | 70 | 31.3 |
| sub10 | 5 | 82 | 70 | 94 | 88 | 82 | 88 | 82 | 88 | 88 | 100 | 86.2 |
| imp10 | - | 64 | 40 | 58 | 46 | 40 | 64 | 34 | 82 | 64 | 0 | 49.2 |

3.2 Results and discussion of the evaluation of the proposed authentication algorithm

The proposed authentication algorithm was evaluated by measuring the FRR and the FAR. The relative accuracy of the system was then calculated. FAR is the rate at which a system authorizes an illegitimate user, and FRR is the rate at which a system rejects a legitimate user [38]. For every authentication system, there are four possible outcomes: i) a legitimate user is authorized, denoted as true positive (TP), ii) an illegitimate user is authorized, denoted as false positive (FP), iii) an illegitimate user is rejected, denoted as true negative (TN) and iv) a legitimate user is rejected, denoted as false negative (FN). FRR is the total number of false negatives over the total number of attempts (FN+TP) as expressed by (1):

$$FRR = \frac{FN}{FN+TP} \tag{1}$$

where FAR is the total number of false positives over the total number of impostor attempts (FP+TN) as expressed by (2).

$$FAR = \frac{FP}{FP+TN} \tag{2}$$

The relative accuracy (ACC) of a system is the total number of denied illegitimate attempts (TN) and authorized legitimate attempts (TP) over the total number of all attempts made (FP+FN+TN+TP) as expressed by (3).

$$Accuracy = \frac{TN+TP}{FN+FP+TN+TP} \cdot 100 \tag{3}$$

Results of the evaluation of the proposed authentication algorithm are given in Table 2. As demonstrated in Table 2, 50% of subjects achieved the maximum accuracy of 100% with 0% FAR and FRR. The average accuracy was 97%.

Table 2. Results of the evaluation of the proposed authentication algorithm

| Subject | TP | FN | FP | TN | FAR | FRR | ACC |
|---------|----|----|----|----|-----|-----|-----|
| S1 | 9 | 1 | 1 | 9 | 10 | 10 | 90 |
| S2 | 10 | 0 | 1 | 9 | 10 | 0 | 95 |
| S3 | 10 | 0 | 0 | 10 | 0 | 0 | 100 |
| S4 | 10 | 0 | 0 | 10 | 0 | 0 | 100 |
| S5 | 10 | 0 | 1 | 9 | 10 | 0 | 95 |
| S6 | 10 | 0 | 0 | 10 | 0 | 0 | 100 |
| S7 | 10 | 0 | 1 | 9 | 10 | 0 | 95 |
| S8 | 10 | 0 | 0 | 10 | 0 | 0 | 100 |
| S9 | 10 | 0 | 1 | 9 | 10 | 0 | 95 |
| S10 | 10 | 0 | 0 | 10 | 0 | 0 | 100 |

3.3. Results and discussion of the impact of emotion and exercise on algorithm performance

EEG authentication's sensitivity to emotions is a significant challenge, negatively affecting performance [39]. This study investigated the impact of emotions on authentication accuracy, considering three states: excitement, sadness, and calmness. To alter participants' emotional states, the researcher used video clips from the DEAP project [40]. This study focused on using these videos to change participants' emotions before capturing EEG signals. Two videos from each category ("exciting," "sad," or "calm") were selected based on user ratings. Participants watched one-minute music clips intended to change their emotional state before the authentication process. Table 3 shows the authentication results for subjects affected by these emotions.

Table 3. Authentication results for subjects affected by excitement, sadness, and calmness

| Subject ID | Algorithm scores | | |
|------------|--------------------|------------------|-----------------|
| | Trial 1 excitement | Trial 2 calmness | Trial 3 sadness |
| S1 | 77 | 70 | 70 |
| S2 | 97 | 94 | 88 |
| S3 | 81 | 84 | 90 |
| S4 | 90 | 90 | 95 |
| S5 | 96.3 | 88.8 | 92.5 |
| S6 | 88.8 | 92.5 | 93.3 |
| S7 | 85 | 100 | 100 |
| S8 | 88.75 | 85 | 92.5 |
| S9 | 92.5 | 96.5 | 85 |
| S10 | 82 | 94 | 82 |

From authentication results for subjects affected by excitement, sadness, and calmness, it was observed that there was only a slight difference or no difference at all in average algorithm scores for all three emotions. It is important to note that this slight difference did not necessarily imply that emotions impacted the performance of the algorithm. The difference was caused by how hard the authentication pattern was for the subject as it was observed during the training session that subjects had a challenge in matching their pattern with the pattern previously recorded in the database.

Chuang *et al.* [15], Choktanomsup *et al.* [35], and Uengtrakul *et al.* [36] noted that physical exercises impact brainwave signals, affecting EEG-based authentication algorithms. This study investigated this effect on 10 subjects who participated in previous experiments. Subjects performed rope skipping while wearing a smart bracelet to monitor heart rates, which were compared to the ideal heart rates for their age as recommended by Tanaka *et al.* [41]. After exercising, subjects were immediately authenticated into the system, and their results were recorded. Table 4 presents the authentication results post-exercise.

For a specific subject score obtained from each trial were not consistent. However, this did not imply that exercising affected the scores. The score inconsistency was associated with the complexity of the subject's authentication pattern as discussed previously. It was concluded from the results that physical exercise had no negative impact on the performance of participants but might have had a positive impact if it improved the mental focus of the participants.

Table 4. Authentication results for subjects after performing physical exercises

| Subject | Trial 1 | Trial 2 | Trial 3 | Average |
|---------|---------|---------|---------|---------|
| S1 | 70 | 70 | 77 | 72.3 |
| S2 | 88 | 94 | 97 | 93 |
| S3 | 84 | 87 | 84 | 85 |
| S4 | 90 | 100 | 90 | 93.3 |
| S5 | 92.5 | 100 | 96.3 | 93.6 |
| S6 | 92.5 | 92.5 | 88.8 | 92.5 |
| S7 | 100 | 95 | 100 | 93.3 |
| S8 | 88.8 | 85 | 88.8 | 90 |
| S9 | 92.5 | 92.5 | 96.3 | 93.8 |
| S10 | 94 | 94 | 100 | 90 |

3.4. Summary of results

In terms of authentication performance, the algorithm achieved an average accuracy of 97%, with a FAR of 5% and a FRR of 1%. The average accuracy of the proposed algorithm was, therefore, higher than in some of the reviewed studies. For instance, Chen *et al.* [17] achieved an accuracy of 86.1% with a FAR of

13.9% and a FRR of 13.9%. Similarly, Gupta *et al.* [14] achieved a true positive rate (TPR) of 92% using supervised classification and 80% using unsupervised classification. Other studies demonstrated accuracy in the range of 97-98% comparable to the one achieved by this study [7], [11], [15], [24]. The method demonstrated robustness against variations in emotional state and physical exercise, maintaining high authentication accuracy. Overall, our findings show that the eye blink-based approach offers superior stability and practicality compared to traditional EEG authentication methods, which often suffer from decreased accuracy due to emotional and physical variations.

4. CONCLUSION AND RECOMMENDATIONS

This study investigated the use of EEG eye blink artifacts as a form of human biometric authentication and developed a corresponding algorithm. The performance of the proposed authentication algorithm was evaluated FAR, FRR, and ACC. The effect of emotions and exercise on the algorithm's performance was also examined to validate its practicality. Results indicated that emotions and exercise had no significant impact on the participants' performance. The study achieved an FRR of 1%, a FAR of 5%, and an ACC of 97%, demonstrating the superior performance of the proposed authentication algorithm compared to other related studies.

Our findings have significant implications for the field of biometric authentication. The high accuracy rate of 97% suggests that EEG eye blink artifacts can be a reliable method for user authentication. The study also identified areas for improvement and practical recommendations to enhance the overall accuracy of the authentication algorithm. Firstly, providing training sessions to users can improve their authentication results, as evidenced by the highest scores recorded in the last three trials. Secondly, adjusting the threshold for acceptance or rejection from the initial value of 70 can help reduce false positives as users become more familiar with their authentication patterns. Finally, using a recording device with more electrodes in the frontal lobe can increase blink detection accuracy, making it easier for subjects to repeat their authentication patterns consistently.

These recommendations not only improve the current algorithm but also suggest potential extensions for future research. Investigating the use of more advanced EEG recording devices and exploring additional biometric modalities could further enhance the reliability and applicability of this authentication method. Overall, our study contributes to the research field by demonstrating the practicality and effectiveness of EEG eye blink artifacts in biometric authentication and provides a foundation for future innovations in this area.

REFERENCES





- [1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.
- [2] V. H. C. De Albuquerque, R. Damaševičius, J. M. R. S. Tavares, and P. R. Pinheiro, "EEG-based biometrics: challenges and applications," *Computational Intelligence and Neuroscience*, vol. 2018, pp. 1–2, Jun. 2018, doi: 10.1155/2018/5483921.
- [3] R. Palaniappan and D. P. Mandic, "EEG based biometric framework for automatic identity verification," *The Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology*, vol. 49, no. 2, pp. 243–250, Nov. 2007, doi: 10.1007/s11265-007-0078-1.
- [4] M. Bassi and P. Triverbi, "Human biometric identification through brain print," in *Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018*, Mar. 2018, pp. 1514–1518, doi: 10.1109/ICECA.2018.8474646.
- [5] A. H. Attia and A. M. Said, "Brain seizures detection using machine learning classifiers based on electroencephalography signals: a comparative study," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 2, pp. 803–810, Aug. 2022, doi: 10.11591/ijeecs.v27.i2.pp803-810.
- [6] E. Niedermeyer and F. H. L. da Silva, "Electroencephalography: basic principles, clinical applications, and related fields." Lippincott Williams & Wilkins, Philadelphia, 2005.
- [7] D. La Rocca *et al.*, "Human brain distinctiveness based on EEG spectral coherence connectivity," *IEEE Transactions on Biomedical Engineering*, vol. 61, no. 9, pp. 2406–2412, Sep. 2014, doi: 10.1109/TBME.2014.2317881.
- [8] S. Marcel and J. del R. Millan, "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 743–748, Apr. 2007, doi: 10.1109/TPAMI.2007.1012.
- [9] G. Buzsáki, C. A. Anastassiou, and C. Koch, "The origin of extracellular fields and currents-EEG, ECoG, LFP, and spikes," *Nature Reviews Neuroscience*, vol. 13, no. 6, pp. 407–420, Jun. 2012, doi: 10.1038/nrn3241.
- [10] P. S. Lamba and D. Virmani, "Information retrieval from emotions and eye blinks with help of sensor nodes," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 4, pp. 2433–2441, Aug. 2018, doi: 10.11591/ijece.v8i4.pp2433-2441.
- [11] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A novel biometric approach for human identification and verification using eye blinking signal," *IEEE Signal Processing Letters*, vol. 22, no. 7, pp. 876–880, Jul. 2015, doi: 10.1109/LSP.2014.2374338.
- [12] J. Espinosa, B. Domenech, C. Vázquez, J. Pérez, and D. Mas, "Blinking characterization from high speed video records. Application to biometric authentication," *PLoS ONE*, vol. 13, no. 5, p. e0196125, May 2018, doi: 10.1371/journal.pone.0196125.
- [13] A. Jalilifard *et al.*, "Use of spontaneous blinking for application in human authentication," *Engineering Science and Technology, an International Journal*, vol. 23, no. 4, pp. 903–910, Aug. 2020, doi: 10.1016/j.jestch.2020.05.007.

- [14] E. Gupta, M. Agarwal, and R. Sivakumar, "Blink to get in: biometric authentication for mobile devices using EEG signals," in *IEEE International Conference on Communications*, Jun. 2020, vol. 2020-June, pp. 1–6, doi: 10.1109/ICC40277.2020.9148741.
- [15] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I think, therefore i am: usability and security of authentication using brainwaves," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7862 LNCS, 2013, pp. 1–16.
- [16] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A new biometric modality for human authentication using eye blinking," in *Proceedings of the 7th Cairo International Biomedical Engineering Conference, CIBEC 2014*, Dec. 2015, pp. 174–177, doi: 10.1109/CIBEC.2014.7020949.
- [17] Y. Chen *et al.*, "A High-Security EEG-based login system with RSVP stimuli and dry electrodes," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2635–2647, Dec. 2016, doi: 10.1109/TIFS.2016.2577551.
- [18] S. H. Liew, Y. H. Choo, Y. F. Low, and Z. I. M. Yusoh, "EEG-based biometric authentication modelling using incremental fuzzy-rough nearest neighbour technique," *IET Biometrics*, vol. 7, no. 2, pp. 145–152, Mar. 2018, doi: 10.1049/iet-bmt.2017.0044.
- [19] F. Balci, "DM-EEGID: EEG-based biometric authentication system using hybrid attention-based LSTM and MLP Algorithm," *Traitement du Signal*, vol. 40, no. 1, pp. 65–79, Feb. 2023, doi: 10.18280/ts.400106.
- [20] L. Hernández-Álvarez, E. Barbierato, S. Caputo, L. Mucchi, and L. H. Encinas, "EEG authentication system based on one- and multi-class machine learning classifiers," *Sensors*, vol. 23, no. 1, p. 186, Dec. 2023, doi: 10.3390/s23010186.
- [21] H. Y. Yap, Y.-H. Choo, Z. I. Mohd Yusoh, and W. H. Khoh, "An evaluation of transfer learning models in EEG-based authentication," *Brain Informatics*, vol. 10, no. 1, p. 19, Dec. 2023, doi: 10.1186/s40708-023-00198-4.
- [22] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A new multi-level approach to EEG based human authentication using eye blinking," *Pattern Recognition Letters*, vol. 82, pp. 216–225, Oct. 2016, doi: 10.1016/j.patrec.2015.07.034.
- [23] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "CEREBRE: a novel method for very high accuracy event-related potential biometric identification," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1618–1629, Jul. 2016, doi: 10.1109/TIFS.2016.2543524.
- [24] Q. Wu, Y. Zeng, C. Zhang, L. Tong, and B. Yan, "An EEG-based person authentication system with open-set capability combining eye blinking signals," *Sensors*, vol. 18, no. 2, p. 335, Dec. 2018, [Online]. Available: <https://www.mdpi.com/1424-8220/19/1/6>.
- [25] Y. Zeng *et al.*, "EEG-based identity authentication framework using face rapid serial visual presentation with optimized channels," *Sensors (Switzerland)*, vol. 19, no. 1, p. 6, Dec. 2019, doi: 10.3390/s19010006.
- [26] B. Wu, W. Meng, and W. Y. Chiu, "Towards enhanced EEG-based authentication with motor imagery brain-computer interface," in *ACM International Conference Proceeding Series*, Dec. 2022, pp. 799–812, doi: 10.1145/3564625.3564656.
- [27] M. TajDini, V. Sokolov, I. Kuzminykh, and B. Ghita, "Brainwave-based authentication using features fusion," *Computers and Security*, vol. 129, p. 103198, Jun. 2023, doi: 10.1016/j.cose.2023.103198.
- [28] T. Beyrouth, N. Mostafa, A. Roshdy, A. S. Karar, and S. Alkork, "Review of EEG-based biometrics in 5G-IoT: current trends and future prospects," *Applied Sciences (Switzerland)*, vol. 14, no. 2, p. 534, Jan. 2024, doi: 10.3390/app14020534.
- [29] L. Krishnamoorthy and A. S. Raju, "An ensemble approach for electrocardiogram and lip features based biometric authentication by using grey wolf optimization," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 3, pp. 1524–1535, Mar. 2024, doi: 10.11591/ijeecs.v33.i3.pp1524-1535.
- [30] W. Alsumari, M. Hussain, L. Alshehri, and H. A. Aboalsamh, "EEG-based person identification and authentication using deep convolutional neural network," *Axioms*, vol. 12, no. 1, p. 74, Jan. 2023, doi: 10.3390/axioms12010074.
- [31] F. Al-Shargie, T. B. Tang, and M. Kiguchi, "Assessment of mental stress effects on prefrontal cortical activities using canonical correlation analysis: an fNIRS-EEG study," *Biomedical Optics Express*, vol. 8, no. 5, p. 2583, May 2017, doi: 10.1364/boe.8.002583.
- [32] S. Thejaswini, K. M. Ravi Kumar, S. Rupali, and V. Abijith, "EEG based emotion recognition using wavelets and neural networks classifier," in *SpringerBriefs in Applied Sciences and Technology*, no. 9789811066979, 2018, pp. 101–112.
- [33] Y. Y. Lee and S. Hsieh, "Classifying different emotional states by means of eegbased functional connectivity patterns," *PLoS ONE*, vol. 9, no. 4, p. e95415, Apr. 2014, doi: 10.1371/journal.pone.0095415.
- [34] L. Orgo, M. Bachmann, J. Lass, and H. Hinrikus, "Effect of negative and positive emotions on EEG spectral asymmetry," in *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, Aug. 2015, vol. 2015-November, pp. 8107–8110, doi: 10.1109/EMBC.2015.7320275.
- [35] K. Choktanomsup, W. Charoenwat, and P. Sittiprapaporn, "Changes of EEG power spectrum in moderate running exercises," in *ECTI-CON 2017 - 2017 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, Jun. 2017, pp. 9–12, doi: 10.1109/ECTICon.2017.8096160.
- [36] P. Uengtrakul, S. Lookhanumancho, and P. Sittiprapaporn, "Effect of Qigong exercise indexed by lightweight electroencephalography," in *ECTI-CON 2017 - 2017 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, Jun. 2017, pp. 17–20, doi: 10.1109/ECTICon.2017.8096162.
- [37] O. G. Lins, T. W. Picton, P. Berg, and M. Scherg, "Ocular artifacts in EEG and event-related potentials i: scalp topography," *Brain Topography*, vol. 6, no. 1, pp. 51–63, Sep. 1993, doi: 10.1007/BF01234127.
- [38] S. Sugrim, C. Liu, M. McLean, and J. Lindqvist, "Robust performance metrics for authentication systems," 2019, doi: 10.14722/ndss.2019.23351.
- [39] T. Pham, W. Ma, D. Tran, D. S. Tran, and D. Phung, "A study on the stability of EEG signals for user authentication," in *International IEEE/EMBS Conference on Neural Engineering, NER*, Apr. 2015, vol. 2015-July, pp. 122–125, doi: 10.1109/NER.2015.7146575.
- [40] S. Koelstra *et al.*, "DEAP: A database for emotion analysis; using physiological signals," *IEEE Transactions on Affective Computing*, vol. 3, no. 1, pp. 18–31, Jan. 2012, doi: 10.1109/T-AFFC.2011.15.
- [41] H. Tanaka, K. D. Monahan, and D. R. Seals, "Age-predicted maximal heart rate revisited," *Journal of the American College of Cardiology*, vol. 37, no. 1, pp. 153–156, Jan. 2001, doi: 10.1016/S0735-1097(00)01054-8.





BIOGRAPHIES OF AUTHORS

Thamang Teddy Madile     is a backend engineering developer at Letshego Financial Services Botswana. He holds an M.Sc. in Computer Science from the Botswana International University of Science and Technology (2021) and a B.Sc. in Computer Science Engineering from the University of Sunderland (2014). With a decade of experience in software development, his research interests span biometrics and biometric authentication, the brain-computer interface, the internet of things, image and signal processing, and algorithms. He can be reached at tmadile@gmail.com.



Dr. Hlomani B. Hlomani     is a senior lecturer and the HOD of Computing and Informatics at the Botswana International University of Science and Technology. He holds an undergraduate degree in Information Technology from the Cape Peninsula University of Technology in Cape Town, South Africa. He earned both his M.Sc. and Ph.D. degrees in Computer Science from the University of Guelph, Ontario, Canada, in 2009 and 2014, respectively. His research interests encompass human-computer interaction, artificial intelligence, the Semantic Web, ontologies, knowledge management, and knowledge engineering. He can be reached at hlomanihb@biust.ac.bw.



Prof. Irina Zlotnikova     is a professor in the Department of Computing and Informatics at Botswana International University of Science and Technology, Palapye, Botswana. She holds a specialist degree in electronic engineering and a Ph.D. in solid state, micro-, and nanoelectronics from Voronezh State University, Russia, as well as an Ed.D. in computer science education from Moscow Pedagogical State University, Russia. Her research interests include human-computer interaction, health informatics, digital transformation, emerging technologies, and information systems. Prof. Zlotnikova has been working in various African countries, including Rwanda, Uganda, Tanzania, and Botswana, since 2006. She can be reached at zlotnikovai@biust.ac.bw.